

CCOW Tutorial

Sentillion, Inc.

For more information contact:

978-749-0022

robs@sentillion.com or
markm@sentillion.com

Agenda

15 min	Overview, History, Demonstration
15 min	Context Management Principles
60 min	Architecture for Common Links
20 min	ActiveX/COM Technology Mapping
20 min	Web/HTTP Technology Mapping
50 min	Architecture for Secure Links
20 min	Secure Links for ActiveX Applications
<u>10 min</u>	Wrap-Up, Q&A
3.5 hrs	

Lots of Terms!

Accept, Accept-Conditional	Context participant	Participant coupon
ActiveX	Context subject	Principal interface
Authentication repository	Context item	Private / Public key
Break Link	Corroborating data	RSA
Busy	Digital signature	Secure hash
Chain of trust	Identifier data	Sign-on
Context	Interface	Survey
Component	Interface interrogation	Technology-Neutral
Context Management Arch. (CMA)	Instigator	Use case
Component Object Model (COM)	Mapping agent	User Link
Context change coupon	Message Authentication Code	W3C
Context change transaction	Patient Link	
Context manager	Passcode	

Copyright © 2000 HL7

Copyright © 2000 Sentillion, Inc.



Sentillion
ENABLING INSIGHT

Clinical Context Object Workgroup



- WHAT:** Couple, Coordinate, Synchronize Applications at Point-of-Use.
- HOW:** "Easy" Standards Using Component-Based Technology.
- WHY:** Providers: Flexibility to Choose Applications They Want.
Vendors: Faster to Market with Best-of-Class Solutions.
Everyone: "Out-of-the-Box" Integration.

WHEN: NOW!

Copyright © 2000 Sentillion, Inc.


Sentillion
ENABLING INSIGHT

The Setting

- Multiple disparate applications:
labs, meds, cardiology, scheduling, billing, etc.
- Users in need of easy access to clinical data:
physicians, nurses, therapists, administrators, etc.
- Kiosk as well as personal workstations:
hospitals, clinics, offices, homes, etc.

Common Context

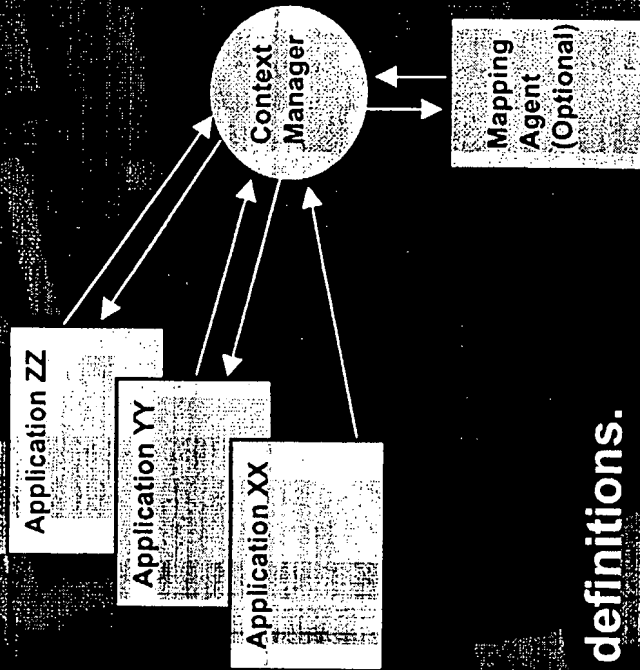
- Eliminates redundant gestures.
- Enables trust.
- Patient Link, User Link, other links.

Copyright © 2000 Sentillion, Inc.



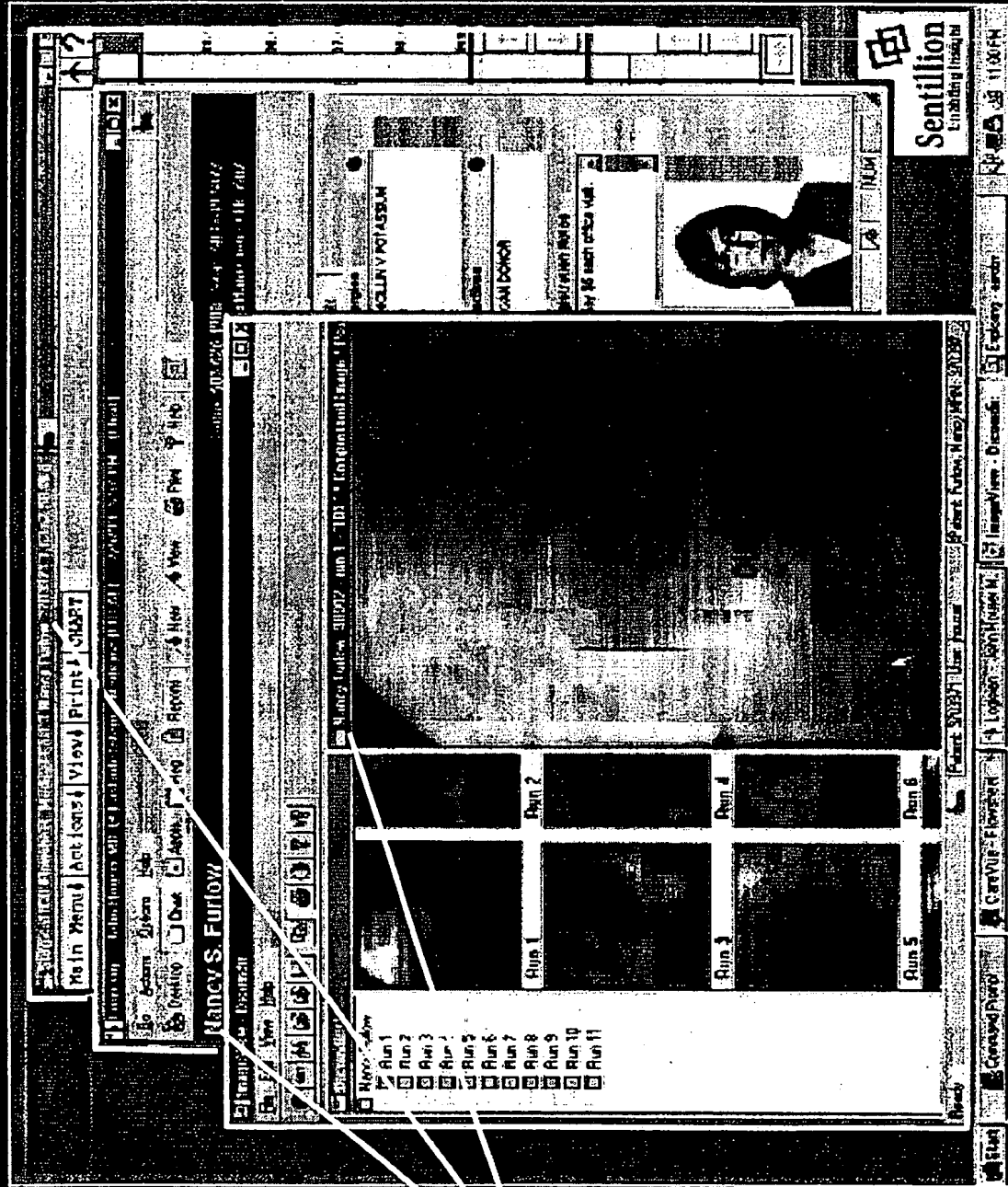
Sentillion
ENABLING INSIGHT

Cinical Links



- Common context data definitions.
- Central context coordinator per desktop.
- Applications don't know about each other.
- Notifications are pushed, data is pulled.

Example: Patient Link



Nancy Furlow



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Demonstration

• Show it.



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Standard Subjects

Ratified as of V1.2:

- User
- Patient
- Encounter

Scheduled in V 1.3:

- Certificate
- Observation

Work in progress:

- Disease state
- Various DICOM subjects
- A moment in time



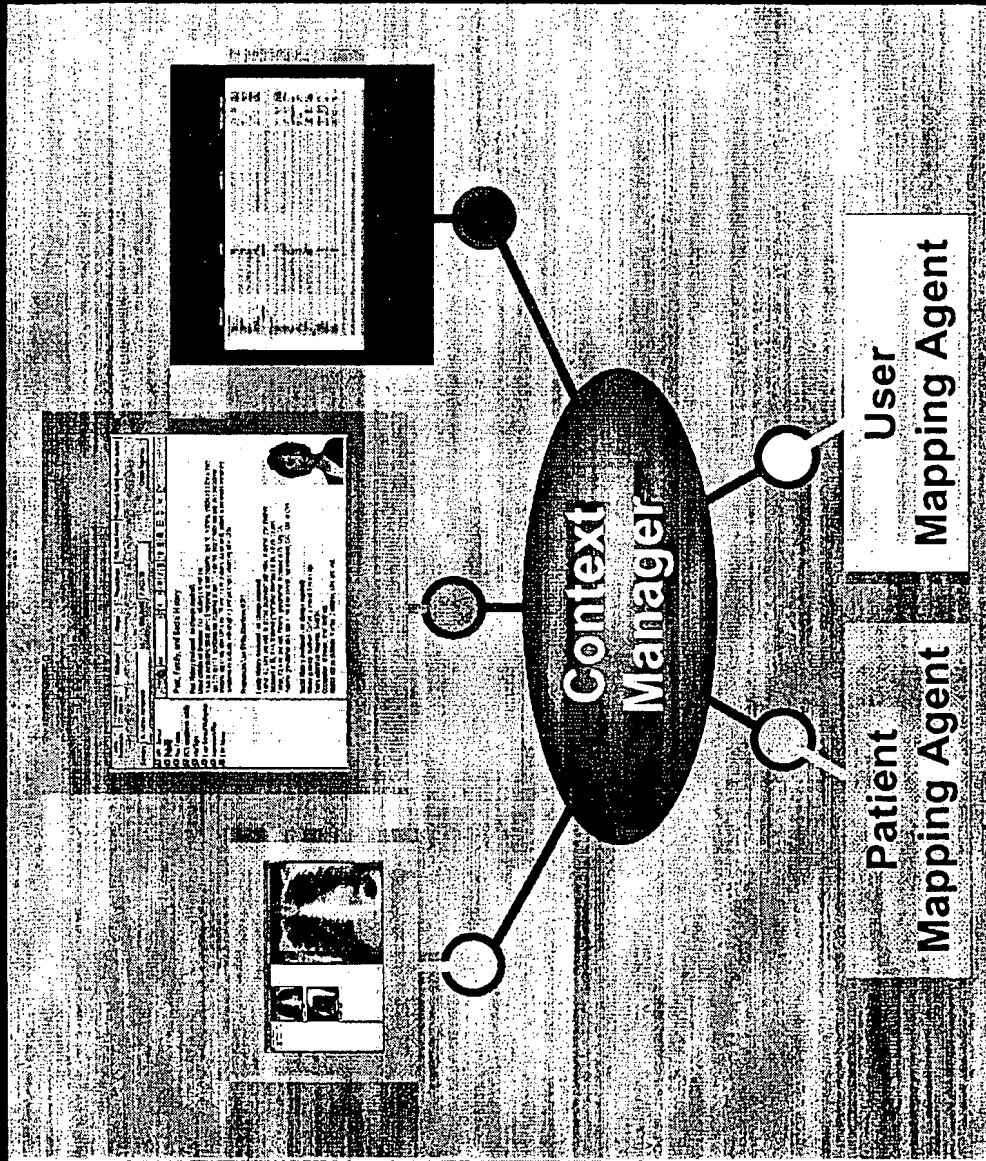
Other Capabilities

- **Secure Subjects** - Only applications with access privileges may set or get (e.g., User)
- **Dependent Subjects** - The value of a subject must be consistent with the value for another subject (e.g., Encounter depends on Patient)
- **Custom Subjects** - May be defined by healthcare providers and/or vendors, distinct from HL7's standard subjects
- **Annotation Subjects** - Data that is in addition to a subject's identity (e.g., a Certificate is an annotation for the User subject)



Architecture

Disparate Applications / CCOW Interfaces

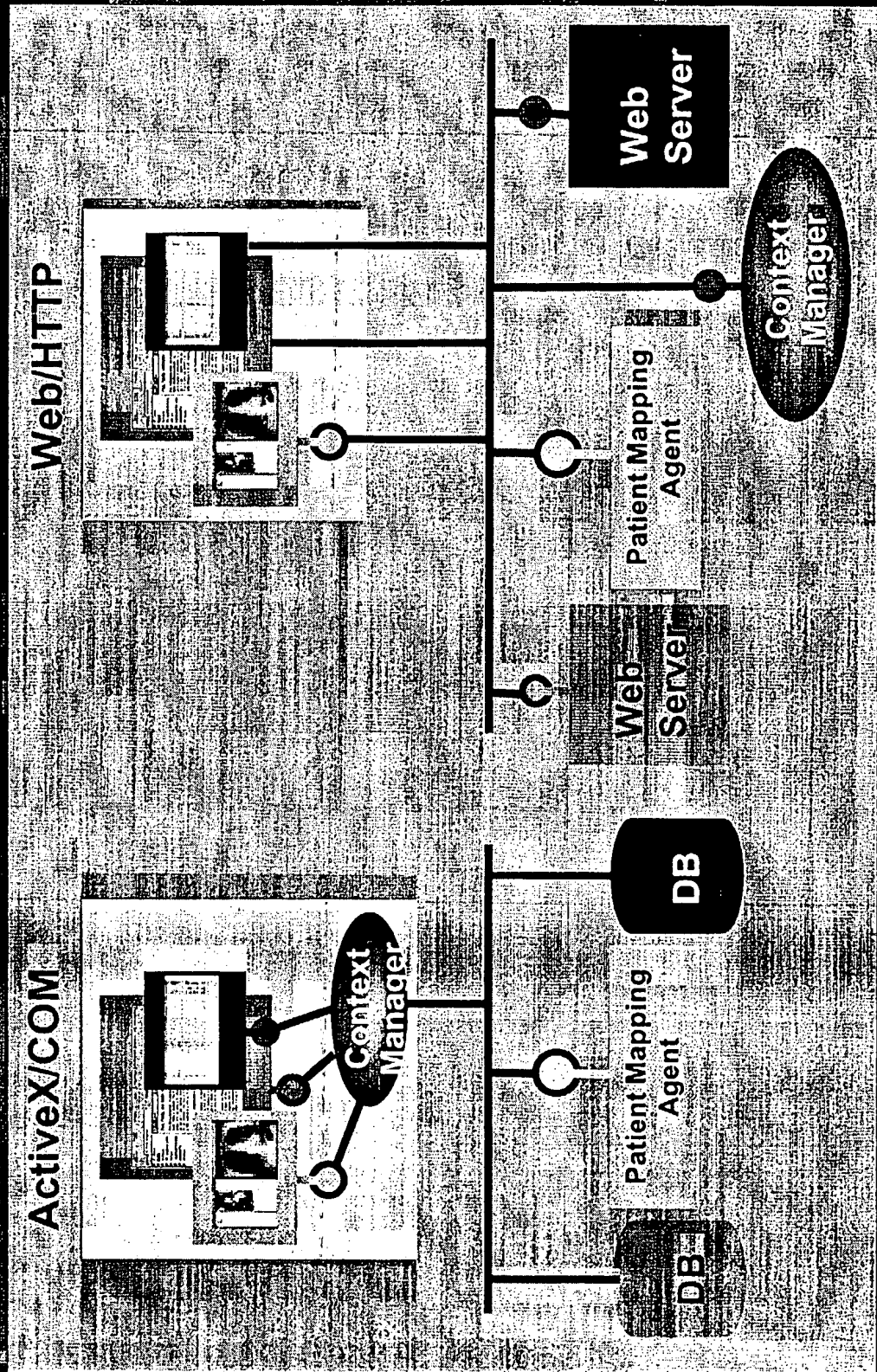


Copyright © 2000 Sentillion, Inc.



Sentillion
ENABLING INSIGHT

Implementations



Sentillion
ENABLING INSIGHT

Some of the Very Active Participants

3M Health Information Systems

Agilent Technologies

Baylor Health Care System

Care Data Systems

Cerner Corporation

Center for Disease Control and Prevention

Community Sector Systems

CoreChange, Inc.

Digineer, Inc.

Duke University Health System

Eclipsis Corporation

Epic Systems Corp

Ernst & Young LLP

GartnerGroup

GE/Marquette Medical Systems

Healthcare.com

Healtheon

Health Network Ventures

Health Patterns, LLC.

MDeverywhere

IBM Global Healthcare

IDX Systems Corporation

Integrated Visions, Inc.

Mayo Foundation

McKessonHBOC

Medic Computer Systems

Medical Manager, Inc.

MedicaLogic

Mortara Instrument, Inc.

NeoTool Development, LLC.

OSF HealthCare System

Oacis Healthcare Systems

Oceania, Inc.

Partners HealthCare System, Inc.

Per Se' Technologies

Pitt County Memorial Hospital

Quadramed

Quantitative Medicine, Inc.

Regenstrief Institute for Health Care

Sentillion, Inc.

Shared Medical Systems Corporation

Spacelab/Burdick

Stockell Healthcare Systems

St. Alphonsus Regional Medical Ctr

Sunquest Information Systems

University of Texas-Houston

Vanderbilt University

VHA Inc.

Copyright © 2000 Sentillion, Inc.



Sentillion

ENABLING INSIGHT

Early Uptake

In Use: Rex (N.C.), Duke (N.C.), Marshfield Clinic (Wisc.), St. Josephs (Wisc.), others

Implementing: St. Alphonsus (Boise), 30+ others early 2001

Shipping Applications: 3M, Agilent, Bionetrix, CoreChange, Care Data Systems, DR Systems, Eclipsys, GE/Marquette, Medscape, McKessonHBOC (soon), Presideo, SpaceLabs/Burdick, Stockell, many others in 2001

Shipping Platform/Tools: Sentillion

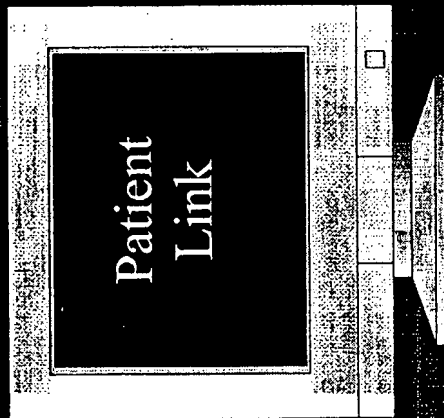
Acceptance: Worldwide (incl. U.S., Canada, Germany, France, Taiwan, Japan)

Copyright © 2000 Sentillion, Inc.



Sentillion
ENABLING INSIGHT

MIE 2000 Demonstration



First Sentient Public Demonstration
 at COM in Chicago

<u>Organization</u>	<u>Component</u>	<u>Technology</u>
Agilent	CareVue (application)	Windows
Charite	MedVision (application)	Windows
GAP	Kauz (application)	Windows
hyperCIS	healthcare One (application)	Web
IMESO	ICU (application)	Windows
Sentillion	Vergence CM (context manager)	Windows + Web



Sentillion
 ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

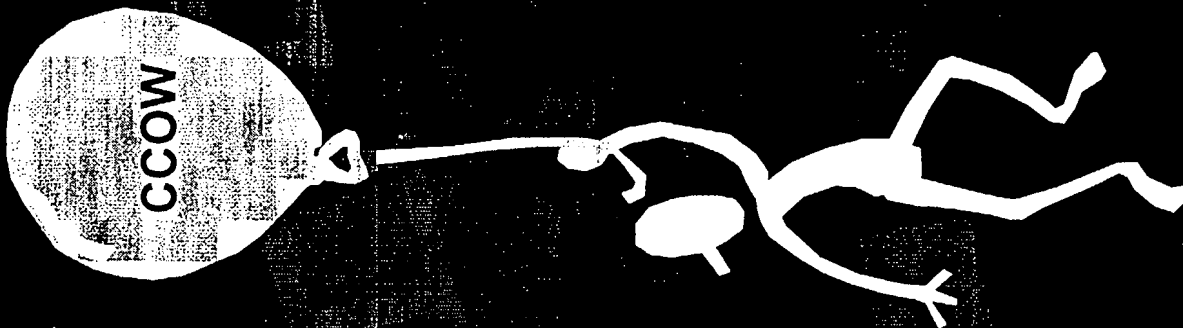
Brief History



- Dec '96 Founded by Wes Rishel
- May '97 First Complete Specification
- Oct '97 Patient Link Demo at MS-HUG '97
- Feb '98 Patient Mapping Agent Demo at HIMSS '98
- Aug '98 CCOW Joins HL7
- Sep '98 User Link Concept Demo at MS-HUG '98
- Feb '99 User Link Demo at HIMSS '99
- Apr '99 HL7 Ratifies "CCOW" 1.0 Specification
- Jul '99 ANSI Certifies "CCOW" 1.0 Specification
- Jan '00 HL7 Ratifies "CCOW" 1.1 Specification
- Mar '00 ANSI Certifies "CCOW" 1.1 Specification
- May '00 CCOW 1.2 Ratified



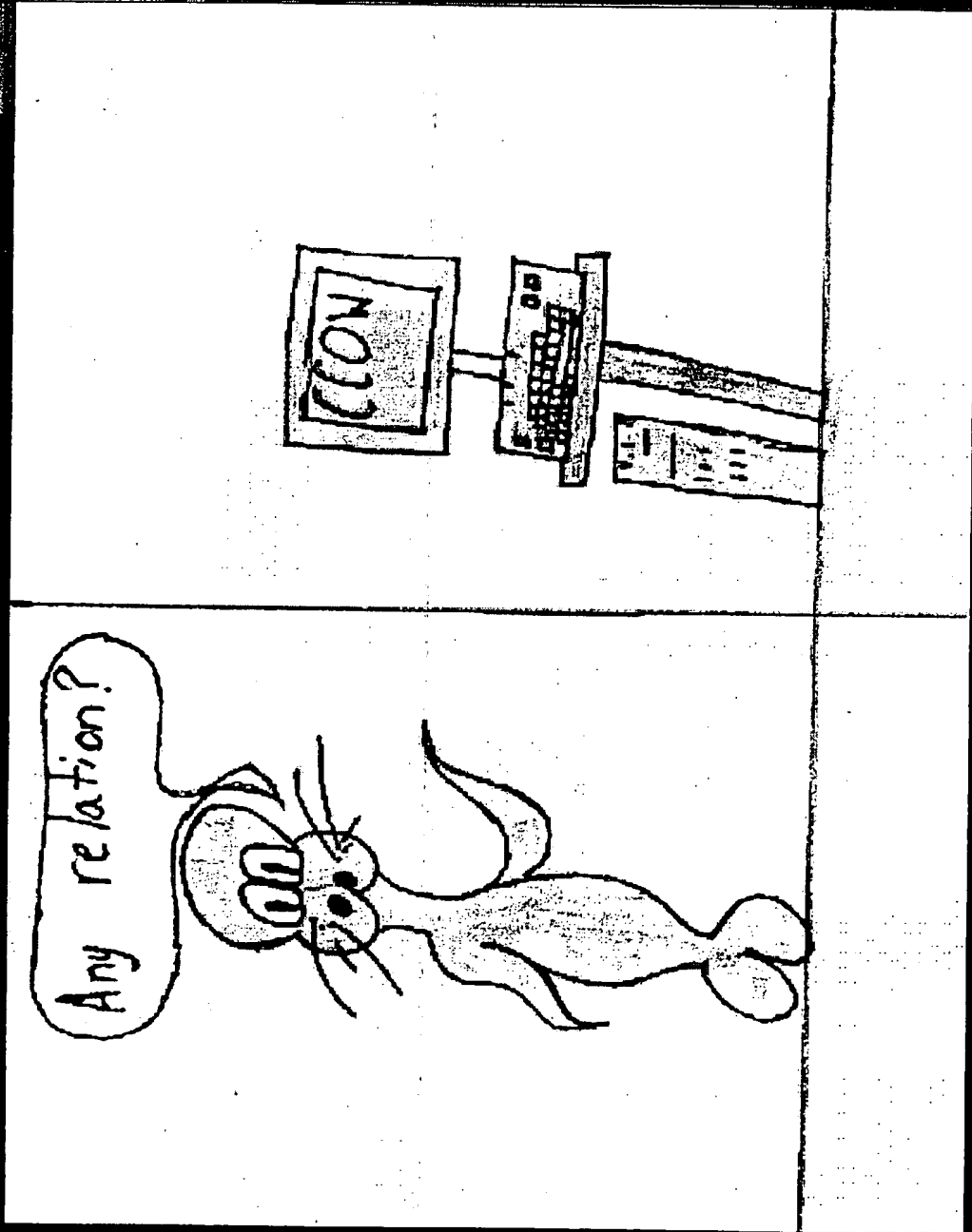
Sentillion
ENABLING INSIGHT




Sentillion
ENABLING INSIGHT

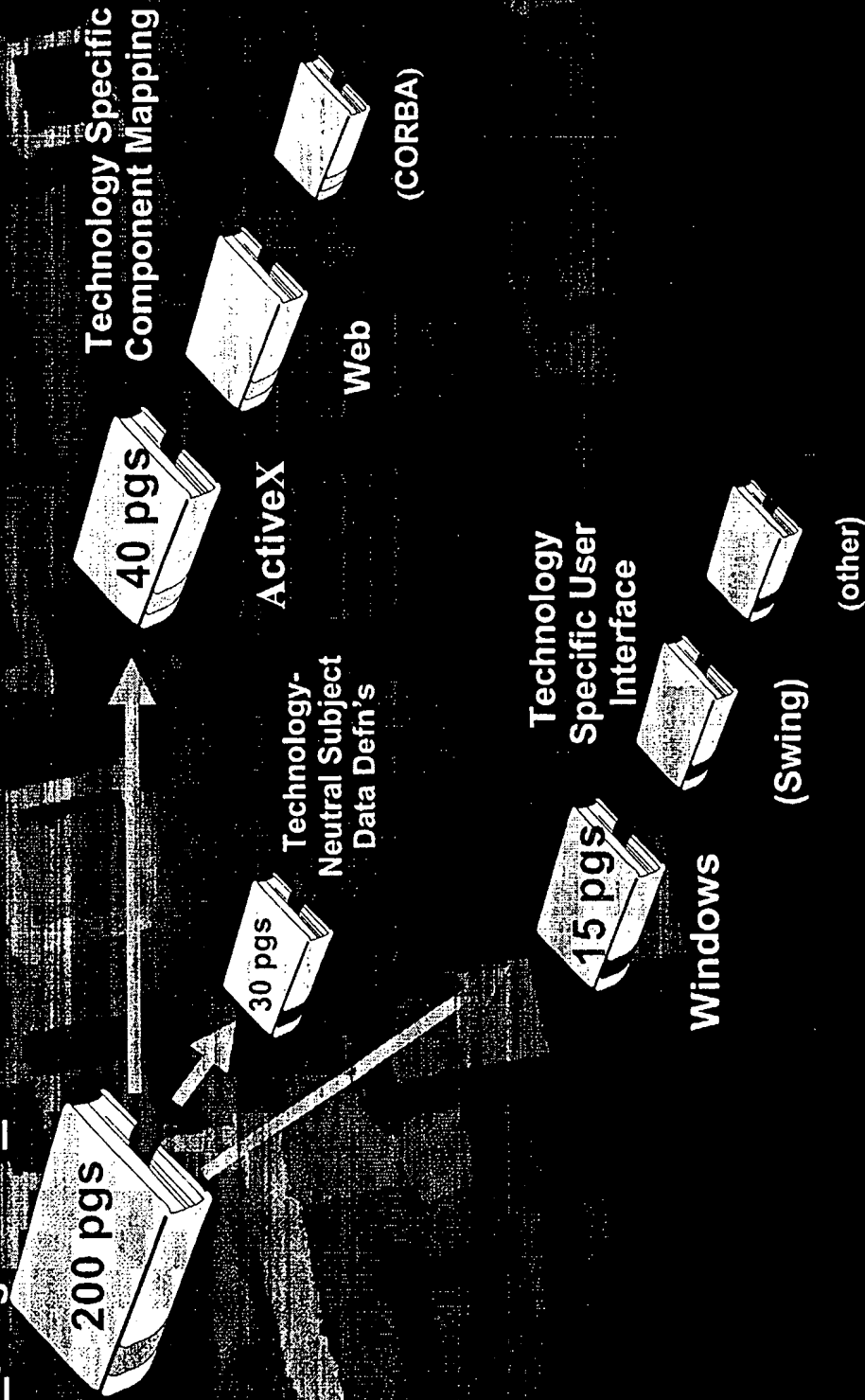
Copyright © 2000 Sentillion, Inc.

CCOW = HL7 SIGVI = CCOW TC



Technology Neutral Standard

Technology Neutral Context
Management Architecture




Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

CCOW Standard Status

1.0 (Ratified April 1999)

- ✓ Component Architecture
- ✓ Common Links: Patient Link
- ✓ Secure Links: User Link
- ✓ Component Interfaces for:
 - Applications
 - Context Manager
 - Patient Mapping Agent
 - User Mapping Agent
 - Authentication Repository
- ✓ Technology Mapping to COM
- ✓ User Interface for Windows

1.1 (Ratified January 2000)

- ✓ Inter-dependent Subjects: Encounter Link
- ✓ Custom Subjects and Items
- ✓ Conformance Statements

1.2 (Ratified May 2000)

- ✓ Technology Mapping to Web

1.3 (Scheduled January 2001)

- ✓ Annotation Agents
- ✓ Observation Link
- ✓ Digital Certificate Annotation

1.4 (Scheduled May 2001)

- ✓ Technology Mapping to SOAP
- ✓ Disease Link
- ✓ DICOM Study Link
- ✓ Multiple Contexts



Principles

- A context subject is an identifiable entity or concept.
- One link, many subjects.
- One authentic source of context data.
- Applications never break their link.
- The user can initiate context change from any application.
- Link status for each application should always be apparent.
- Applications never change the user's "focus."



Architecture

- Central context owner/change coordinator per desktop.
- Applications never know about each other.
- Notifications are pushed, data is pulled.
- Context subject data is a set of related items.
- There are *identifier* and *corroborating* data items.
- Each item is represented as a name/value pair.
- CCOW defines the names and the value data type.
- Item names and data types leveraged from HL7.
- A subject can have multiple synonymous identifiers.

Context
Manager




Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Key Components

Context Manager = Coordinator

Context Participant = Application

Mapping Agent = Identifier Correlation

Item Names

“Subject.Role.Prefix.Suffix”

Subject = Patient or User

Role = id for identifier data
co for corroborating data

Prefix = MRN, Logon, etc.

Suffix = a Site, an Application, an Organization

Item Example

- Identifier Data Item :

Name = Patient.Id.MRN.City_Clinic

Value = RAS-331000344-JHJ-9817238

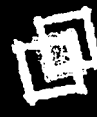
- Corroborating Data Item:

Name = Patient.Co.Name

Value = Seliger^Robert

Custom Subjects/Items

- Add domain name to custom subject name:
implicit - [hl7.org]Patient
explicit - [sentillion.com]Payer
- Add domain name to custom item name:
implicit - Patient.Co.[hl7.org]Name
explicit - Patient.Co.[sentillion.com]MaidenName

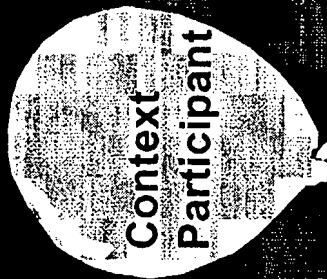


Common Links



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

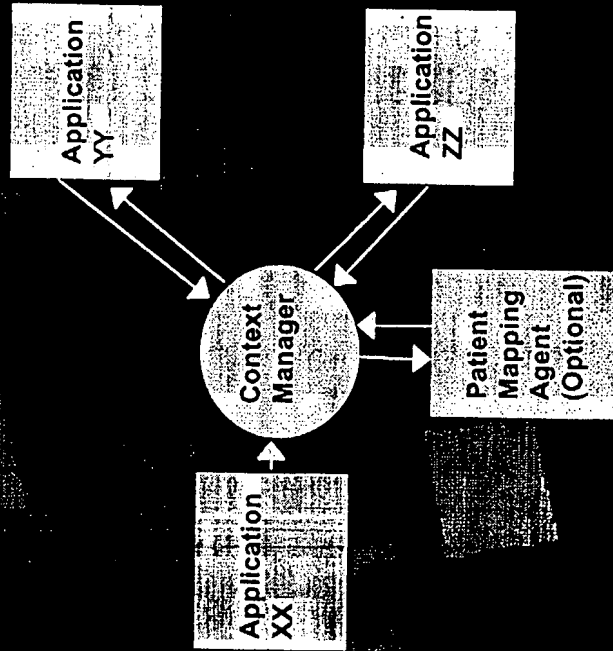


Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

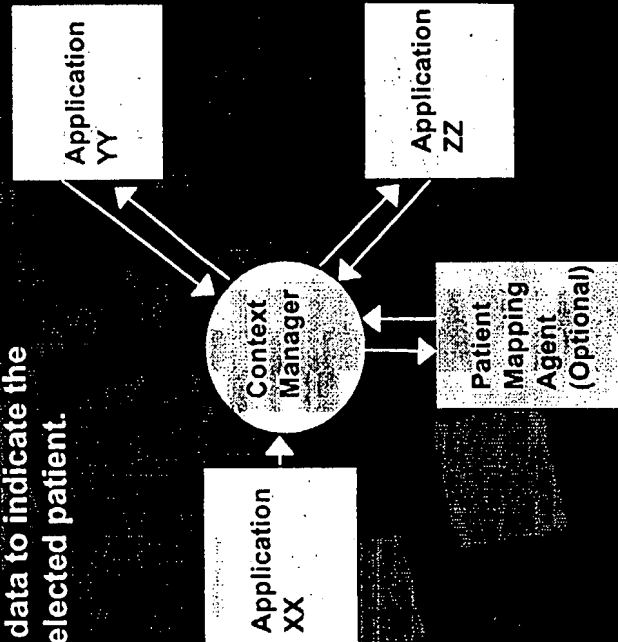
Theory of Operation: Patient Link

(1) User selects
the patient of
interest using any
application on the
clinical desktop.



Theory of Operation: Patient Link

- (1) User selects the patient of interest using any application on the clinical desktop.
- (2) Application tells the context manager to start a context change transaction and sets the context data to indicate the newly selected patient.



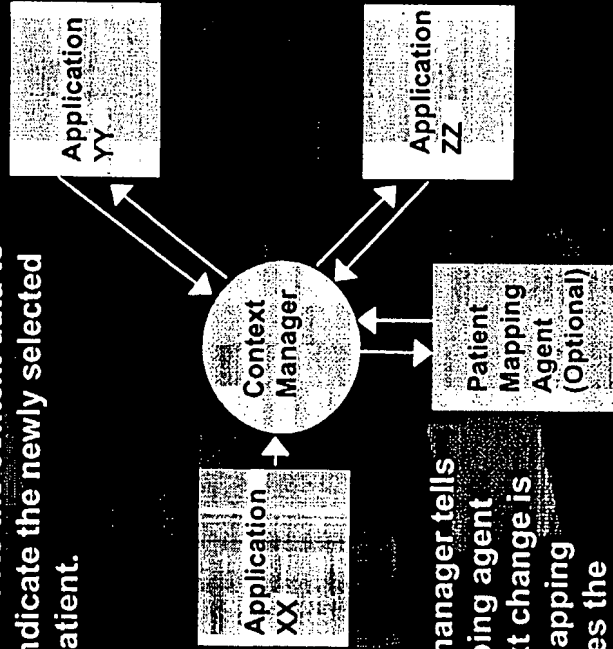
Copyright © 2000 Sentillion, Inc.

Theory of Operation: Patient Link

(1) User selects the patient of interest using any application on the clinical desktop.

(2) Application tells the context manager to start a context change transaction and sets the context data to indicate the newly selected patient.

(3) Context manager tells patient mapping agent that a context change is occurring; mapping agent supplies the context manager with other identifiers by which the patient is known.



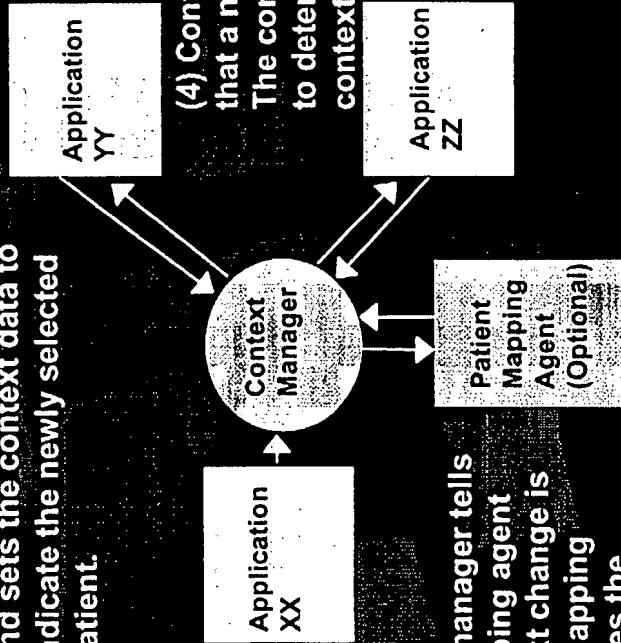
Theory of Operation: Patient Link

(1) User selects the patient of interest using any application on the clinical desktop.

(2) Application tells the context manager to start a context change transaction and sets the context data to indicate the newly selected patient.

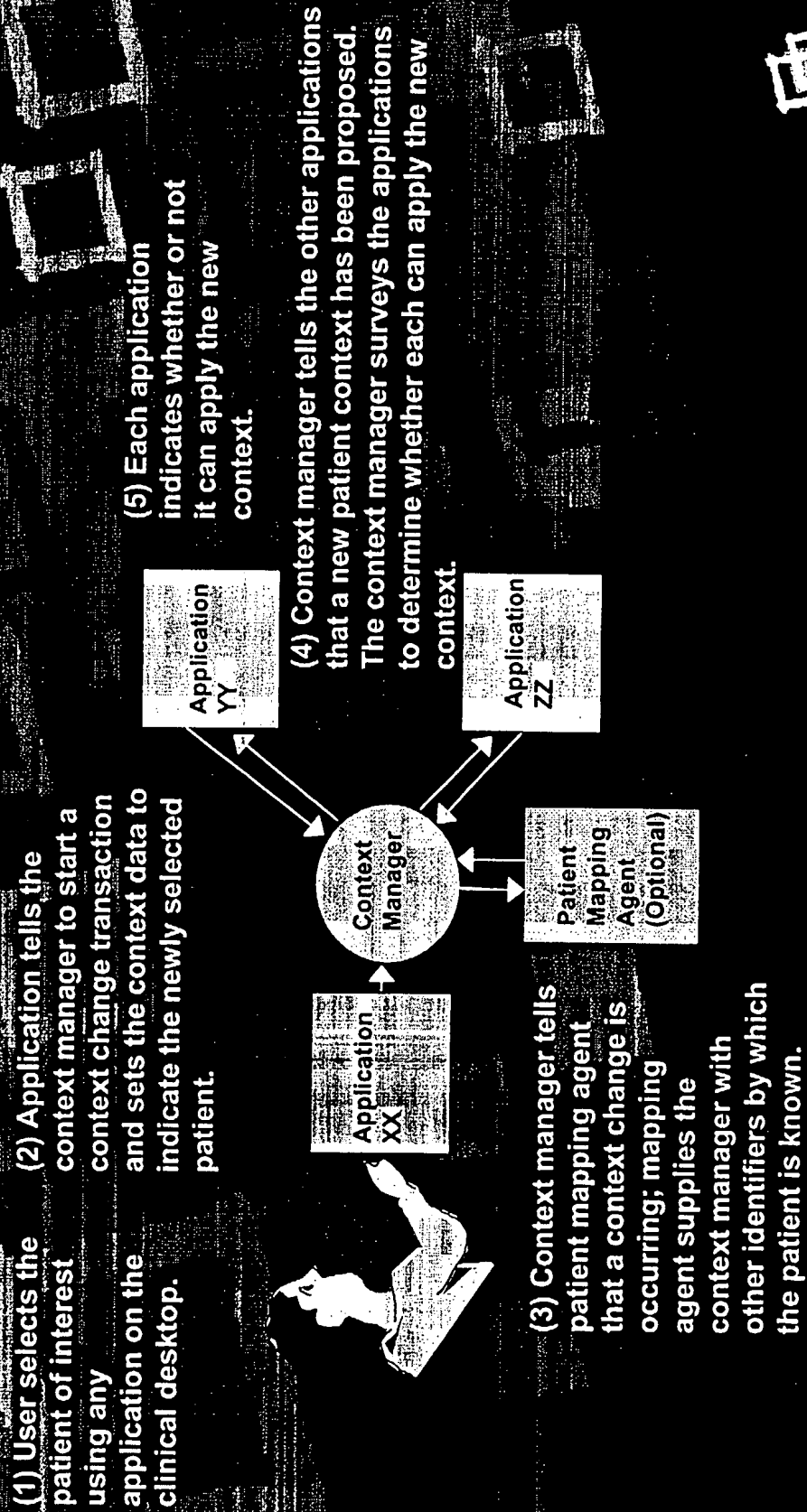


(3) Context manager tells patient mapping agent that a context change is occurring; mapping agent supplies the context manager with other identifiers by which the patient is known.



(4) Context manager tells the other applications that a new patient context has been proposed. The context manager surveys the applications to determine whether each can apply the new context.

Theory of Operation: Patient Link



Theory of Operation: Patient Link

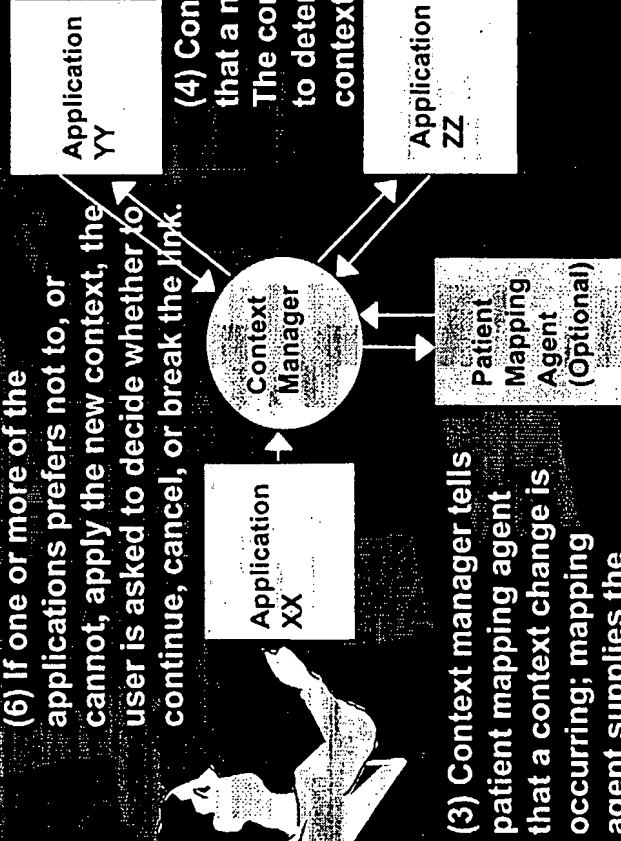
(1) User selects the patient of interest using any application on the clinical desktop.

(2) Application tells the context manager to start a context, change transaction and sets the context data to indicate the newly selected patient.

(6) If one or more of the applications prefers not to, or cannot, apply the new context, the user is asked to decide whether to continue, cancel, or break the link.

(5) Each application indicates whether or not it can apply the new context.

(4) Context manager tells the other applications that a new patient context has been proposed. The context manager surveys the applications to determine whether each can apply the new context.



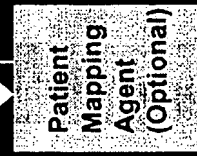
(3) Context manager tells patient mapping agent that a context change is occurring; mapping agent supplies the context manager with other identifiers by which the patient is known.

Theory of Operation: Patient Link

(1) User selects the patient of interest using any application on the clinical desktop.

(2) Application tells the context manager to start a context change transaction and sets the context data to indicate the newly selected patient.

(6) If one or more of the applications prefers not to, or cannot, apply the new context, the user is asked to decide whether to continue, cancel, or break the link.

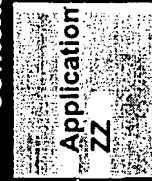


(3) Context manager tells patient mapping agent that a context change is occurring; mapping agent supplies the context manager with other identifiers by which the patient is known.



(5) Each application indicates whether or not it can apply the new context.

(4) Context manager tells the other applications that a new patient context has been proposed. The context manager surveys the applications to determine whether each can apply the new context.



(7) Context manager tells each application to apply the new context, or that the transaction has been canceled.



Sentillion
ENABLING INSIGHT

Theory of Operation: Patient Link

(1) User selects the patient of interest using any application on the clinical desktop.

(2) Application tells the context manager to start a context change transaction and sets the context data to indicate the newly selected patient.

(6) If one or more of the applications prefers not to, or cannot, apply the new context, the user is asked to decide whether to continue, cancel, or break the link.

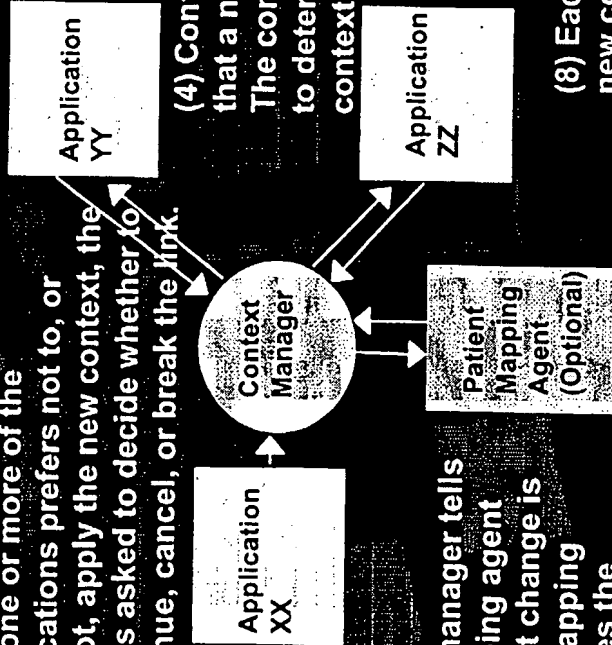


(5) Each application indicates whether or not it can apply the new context.

(4) Context manager tells the other applications that a new patient context has been proposed. The context manager surveys the applications to determine whether each can apply the new context.

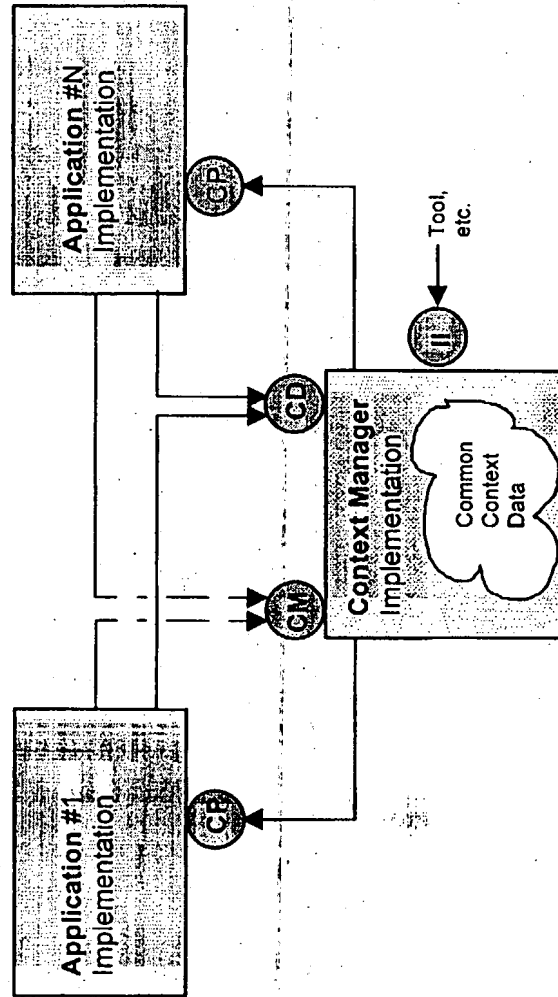
(7) Context manager tells each application to apply the new context, or that the transaction has been canceled.

(8) Each application applies the new context if instructed to do so by the context manager. Each application gets the new patient context from the context manager.



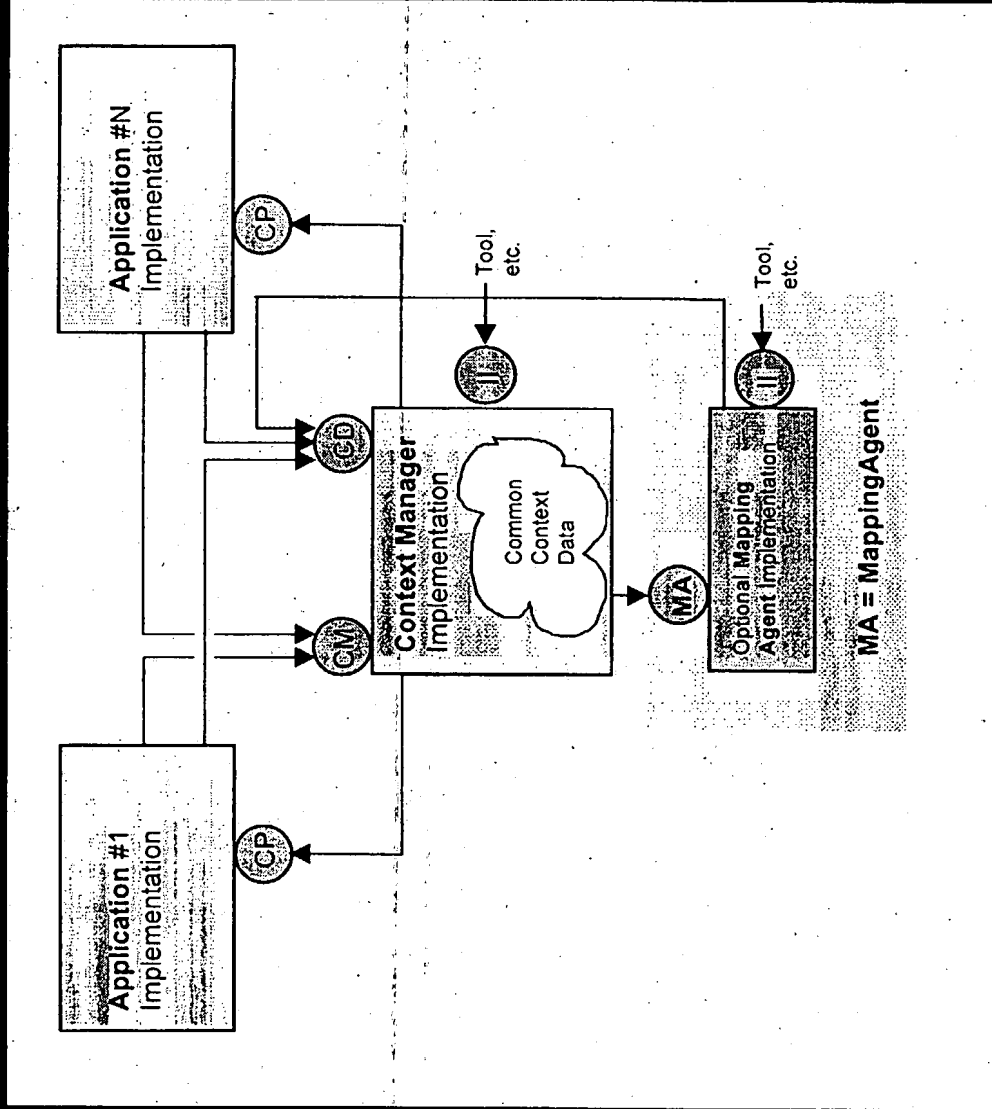
(3) Context manager tells patient mapping agent that a context change is occurring; mapping agent supplies the context manager with other identifiers by which the patient is known.

Architecture



Component Interfaces
 CD = ContextData
 CM = ContextManager
 CP = ContextParticipant
 II = ImplementationInformation

Architecture



Copyright © 2000 Sentillion, Inc.



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Context Data Object

- Contained within central coordinator.
- Maintained by applications.
- Two instances:

Proposed context

Committed context

- Identified by context change coupon.



Interface Definition

example

```
interface ContextParticipant {
```

```
    ContextChangesPending  
    inputs(long contextCoupon)  
    outputs(string decision, string reason)  
    raises()
```

```
    ContextChangesAccepted
```

```
    inputs(long contextCoupon)  
    outputs()  
    raises()
```

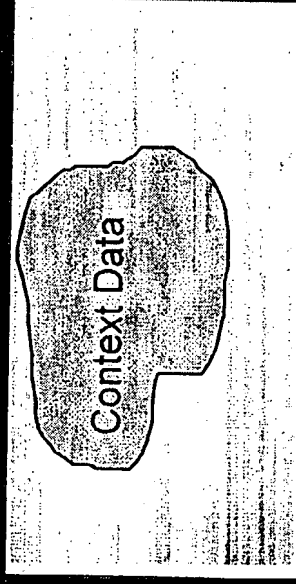
```
    // stuff omitted
```

```
}
```



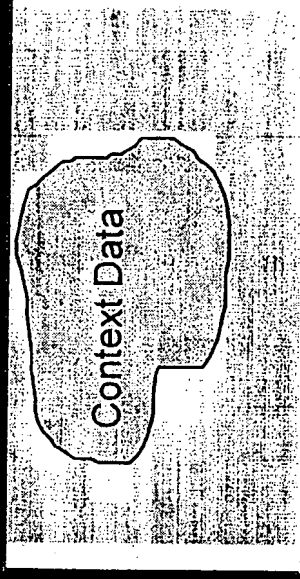
Interface ContextManager

- JoinCommonContext
- LeaveCommonContext
- SuspendParticipation
- ResumeParticipation



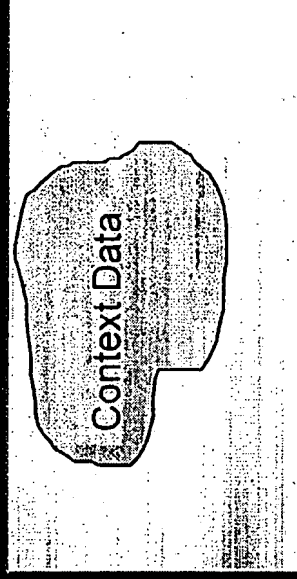
Interface ContextManager

- JoinCommonContext
- LeaveCommonContext
- SuspendParticipation
- ResumeParticipation
- StartContextChanges
- EndContextChanges
- UndoContextChanges
- PublishChangesDecision
- MostRecentContextCoupon



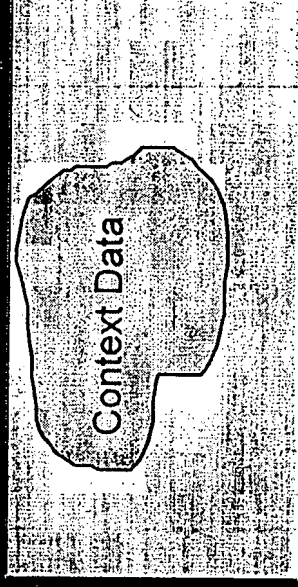
Interface ContextData

- GetItemNames
- GetItemValues
- SetItemValues
- DeleteItems



Interface Implementation Information

- Manufacturer
- PartNumber
- RevMajorNum
- RevMinorNum
- TargetOS
- TargetOSRev
- WhenInstalled

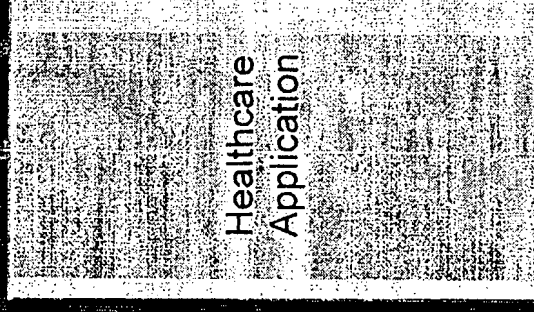


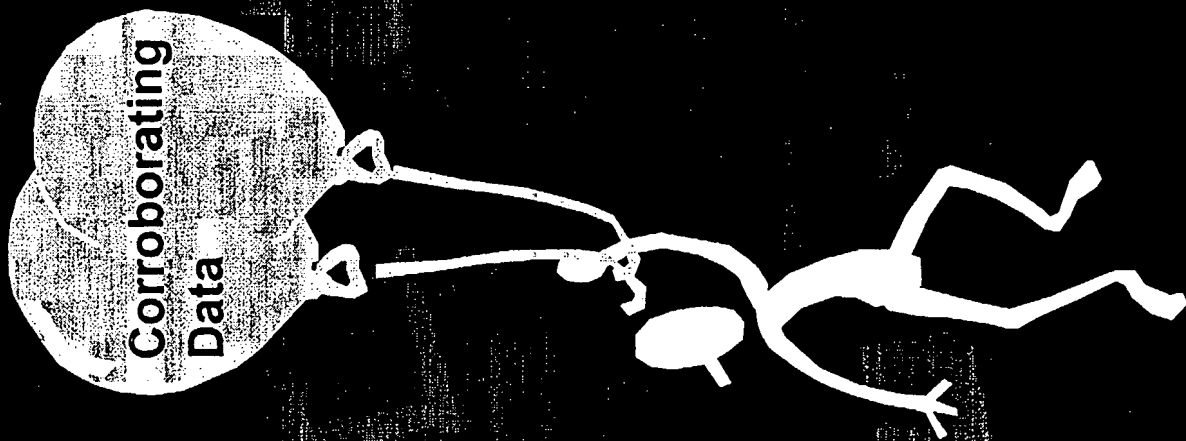
Sentillion
ENABLING INSIGHT

Interface ContextParticipant

- ContextChangesPending
- ContextChangesAccepted
- ContextChangesCanceled
- CommonContextTerminated
- Ping

CP

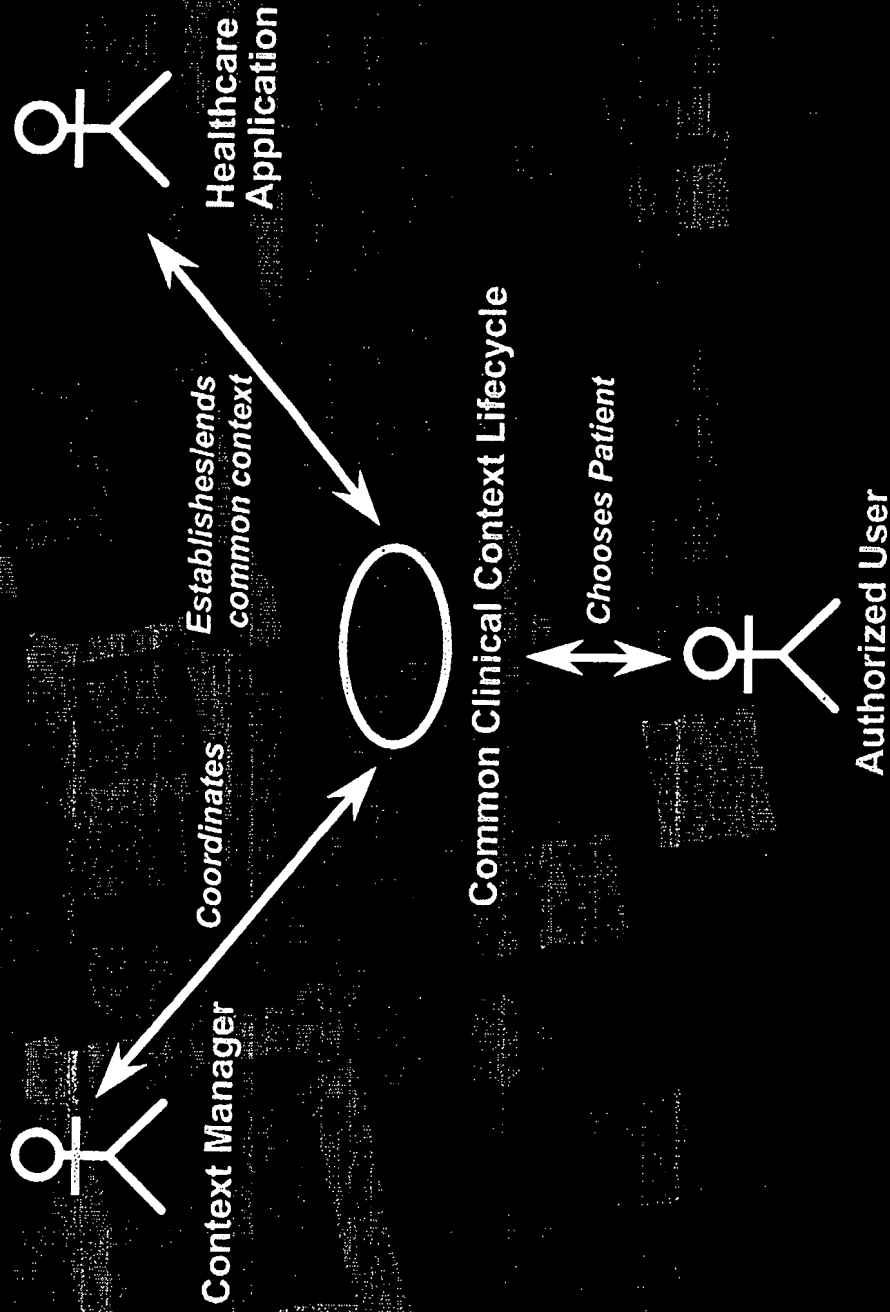





Sentillion
ENABLING INSIGHT

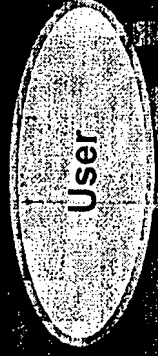
Copyright © 2000 Sentillion, Inc.

Common Context System: Lifecycle Use Case



Copyright © 2000 Sentillion, Inc.

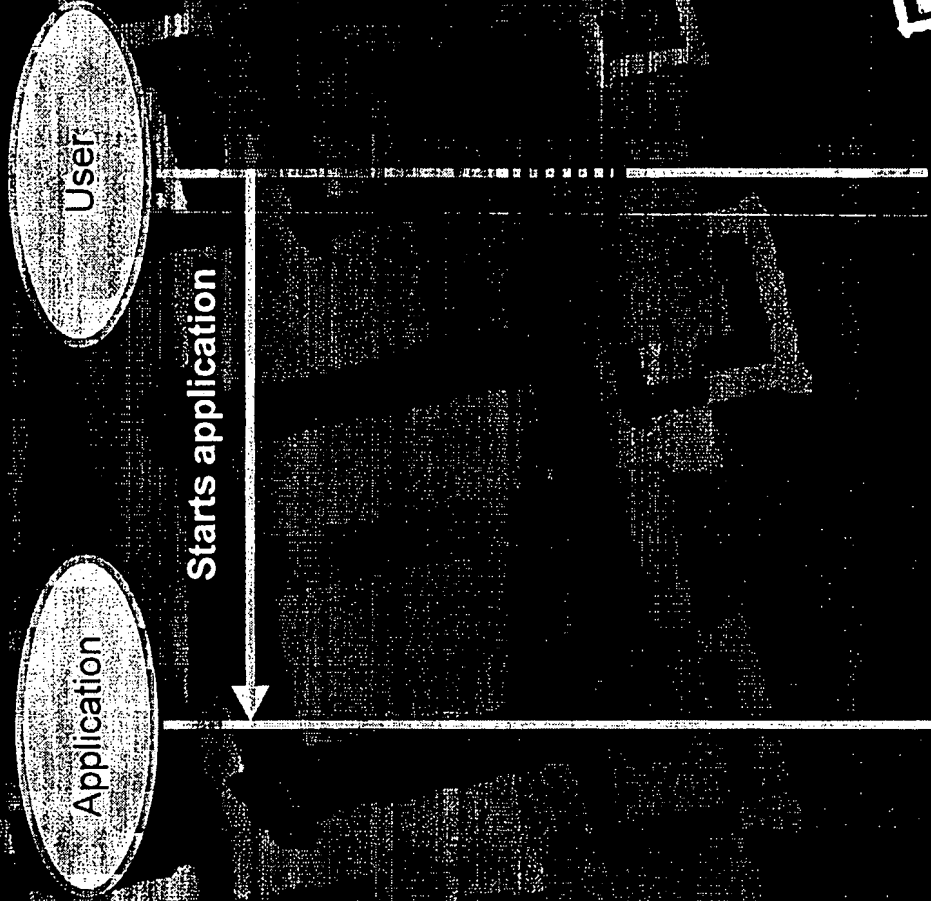
Lifecycle: in the beginning ...



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

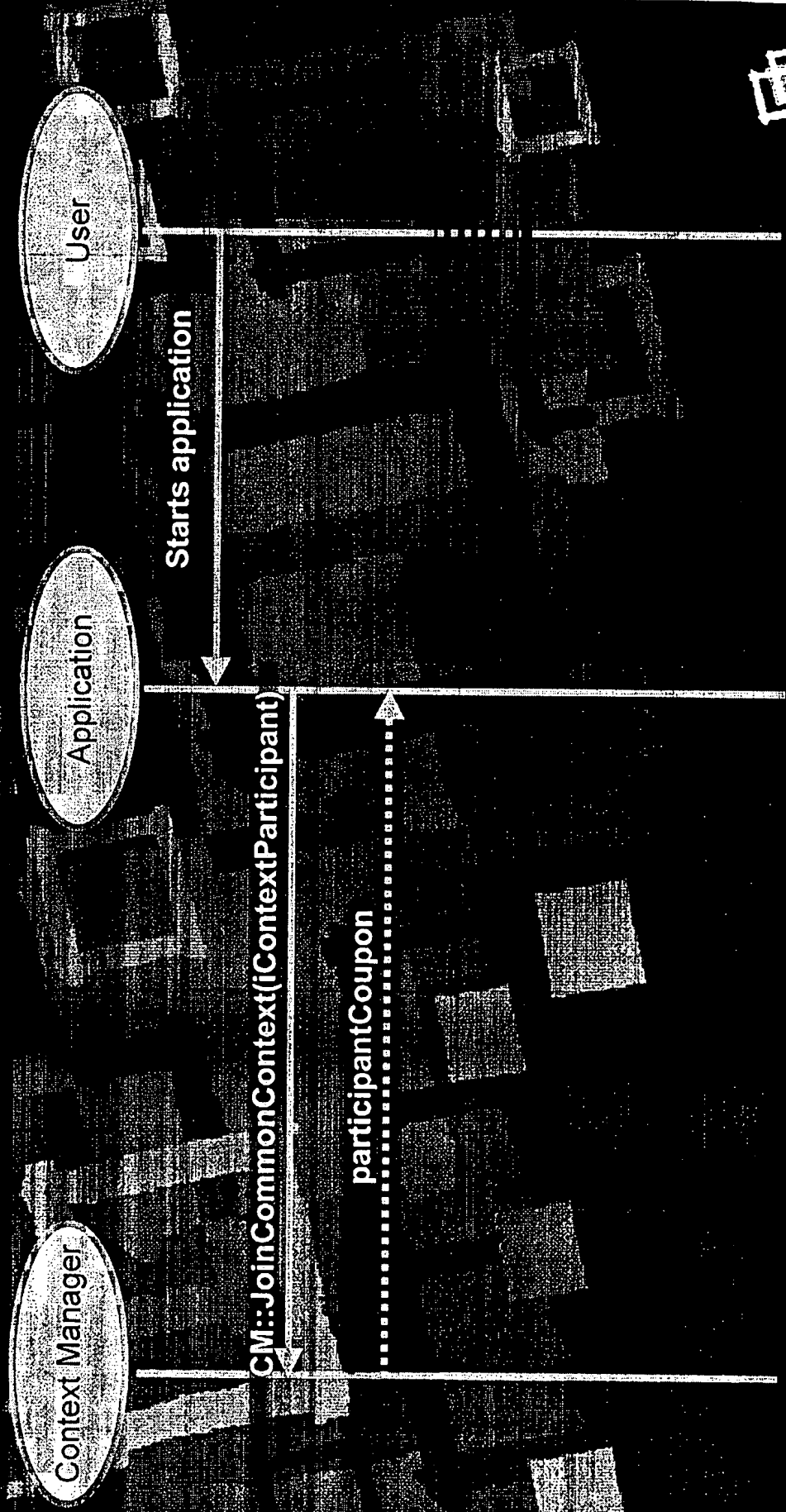
Lifecycle: user starts application



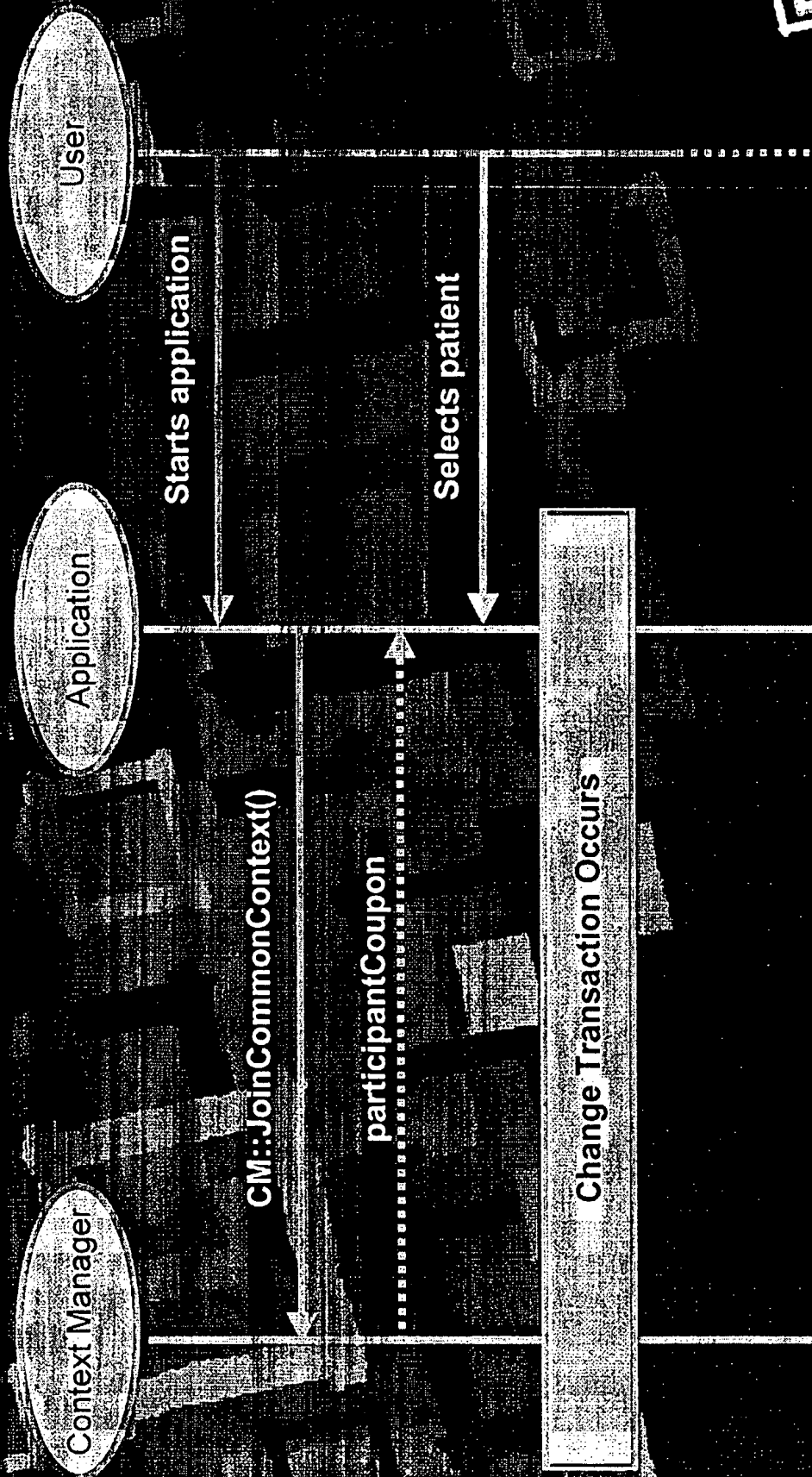
Copyright © 2000 Sentillion, Inc.


Sentillion
ENABLING INSIGHT

Lifecycle: application joins context

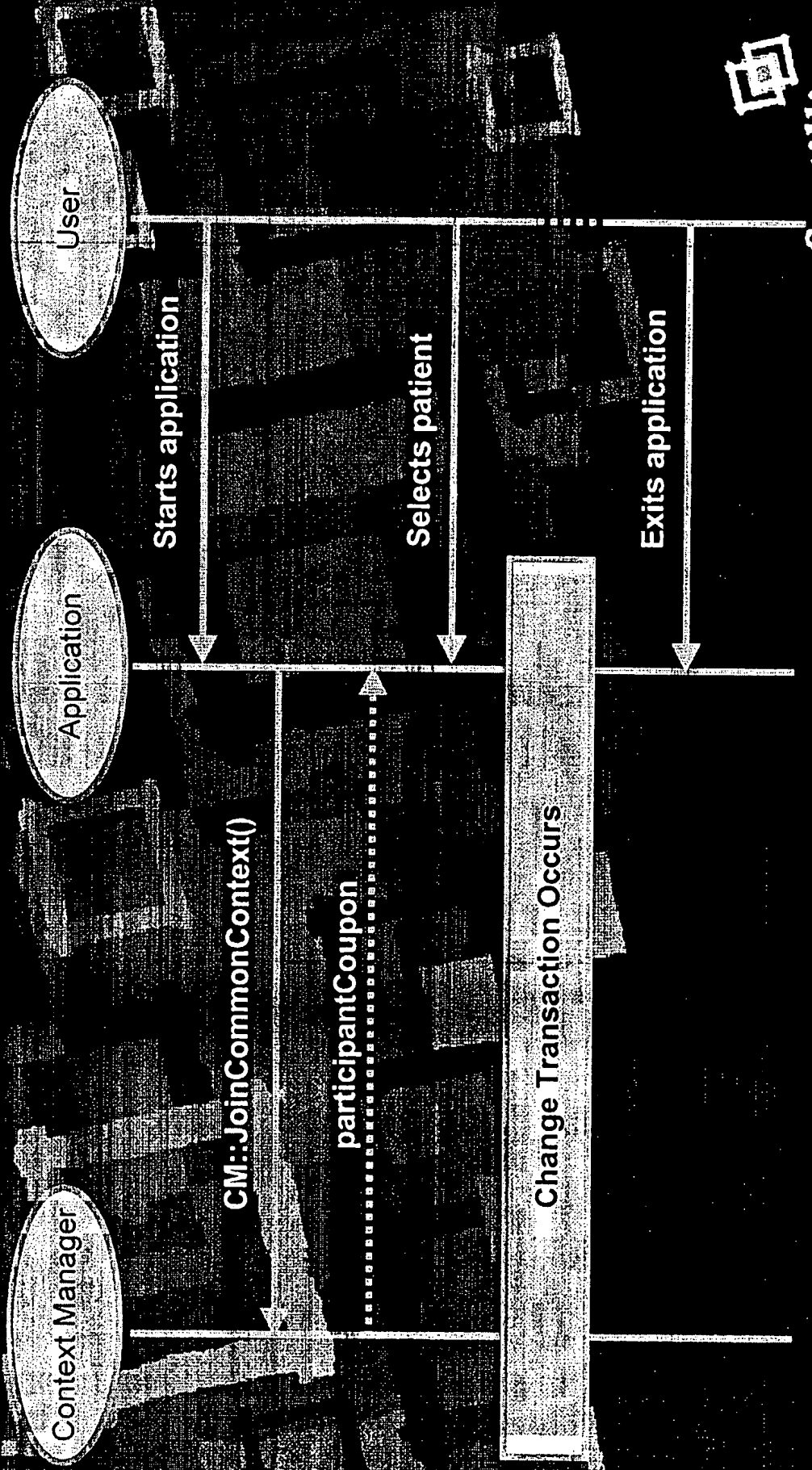


Lifecycle: user sets the context

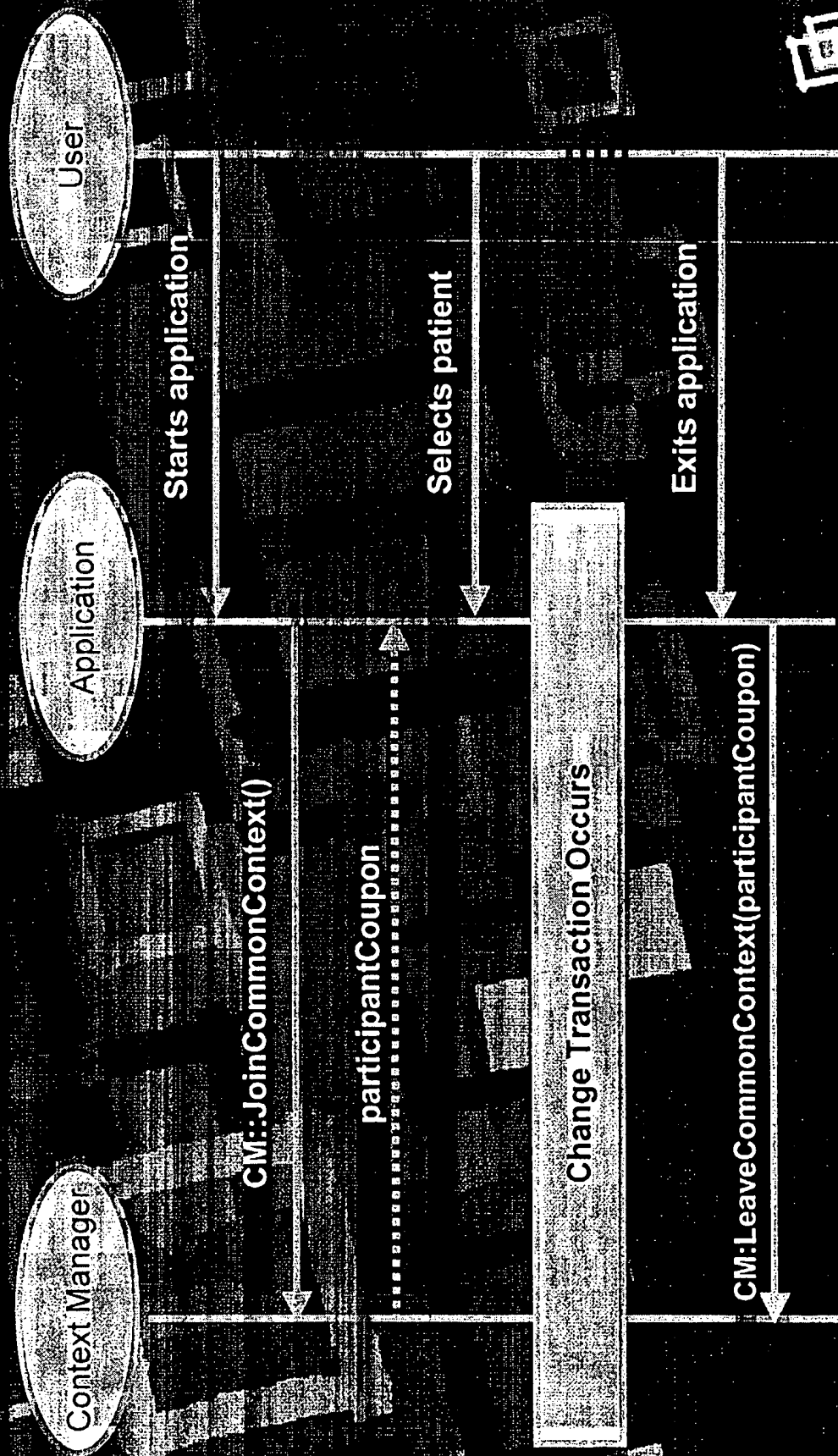


Copyright © 2000 Sentillion, Inc.

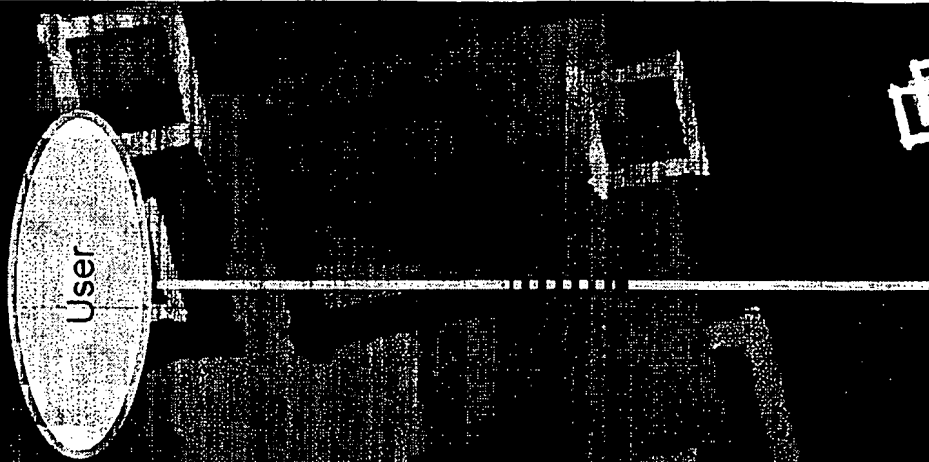
Lifecycle: user exits the application



Lifecycle: application leaves the context



Lifecycle: and in the end ...



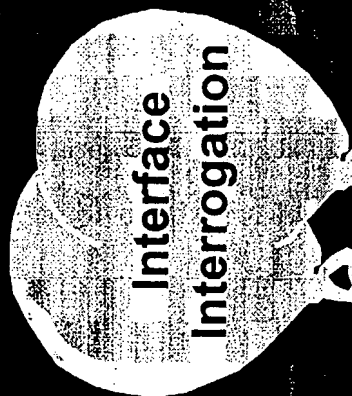
Sentillion

ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Application Behavior Summary: Lifecycle

- Application joins context at startup
- Application denoted by participant coupon.
- Application leaves context prior to exit.

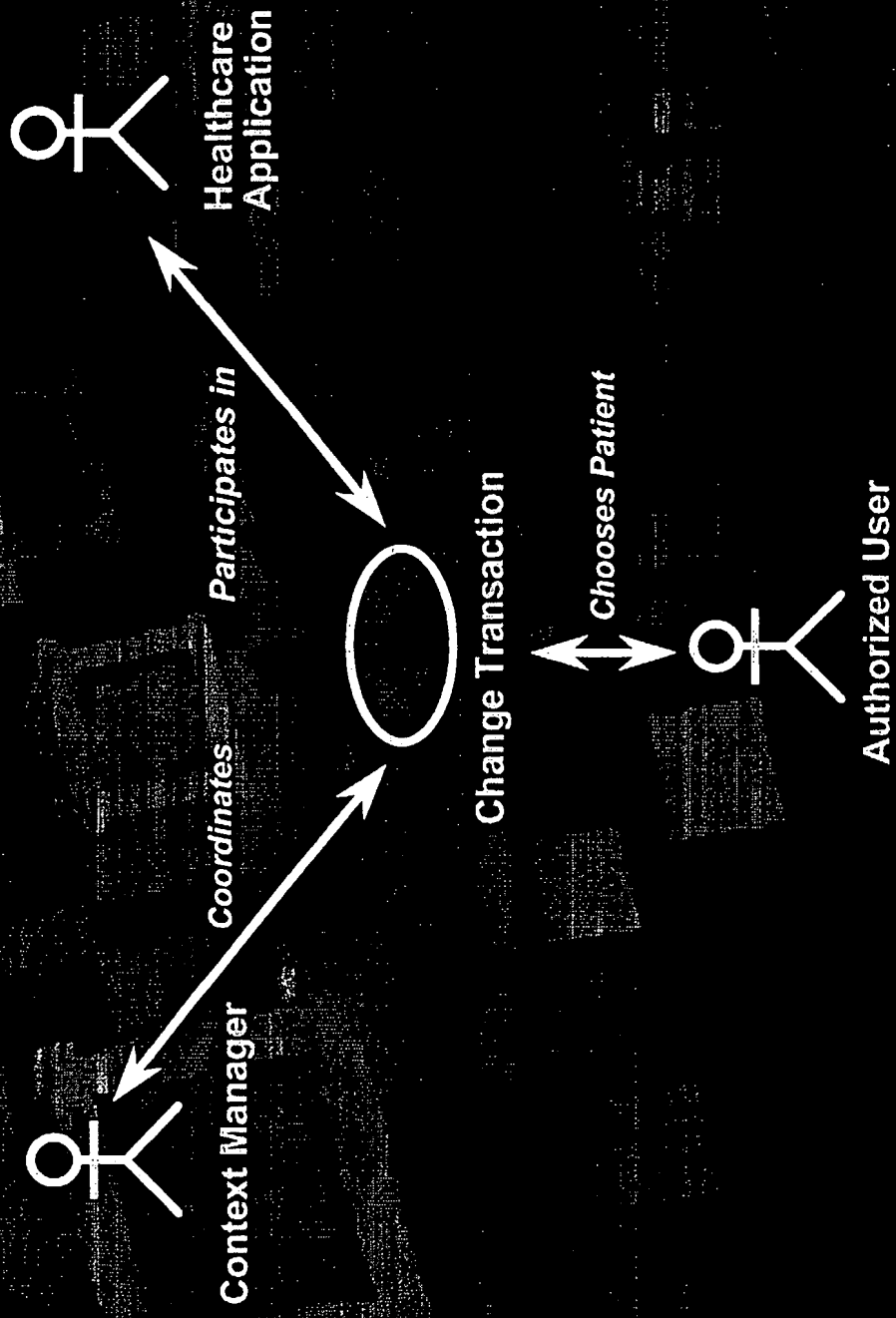


Copyright © 2000 Sentillion, Inc.

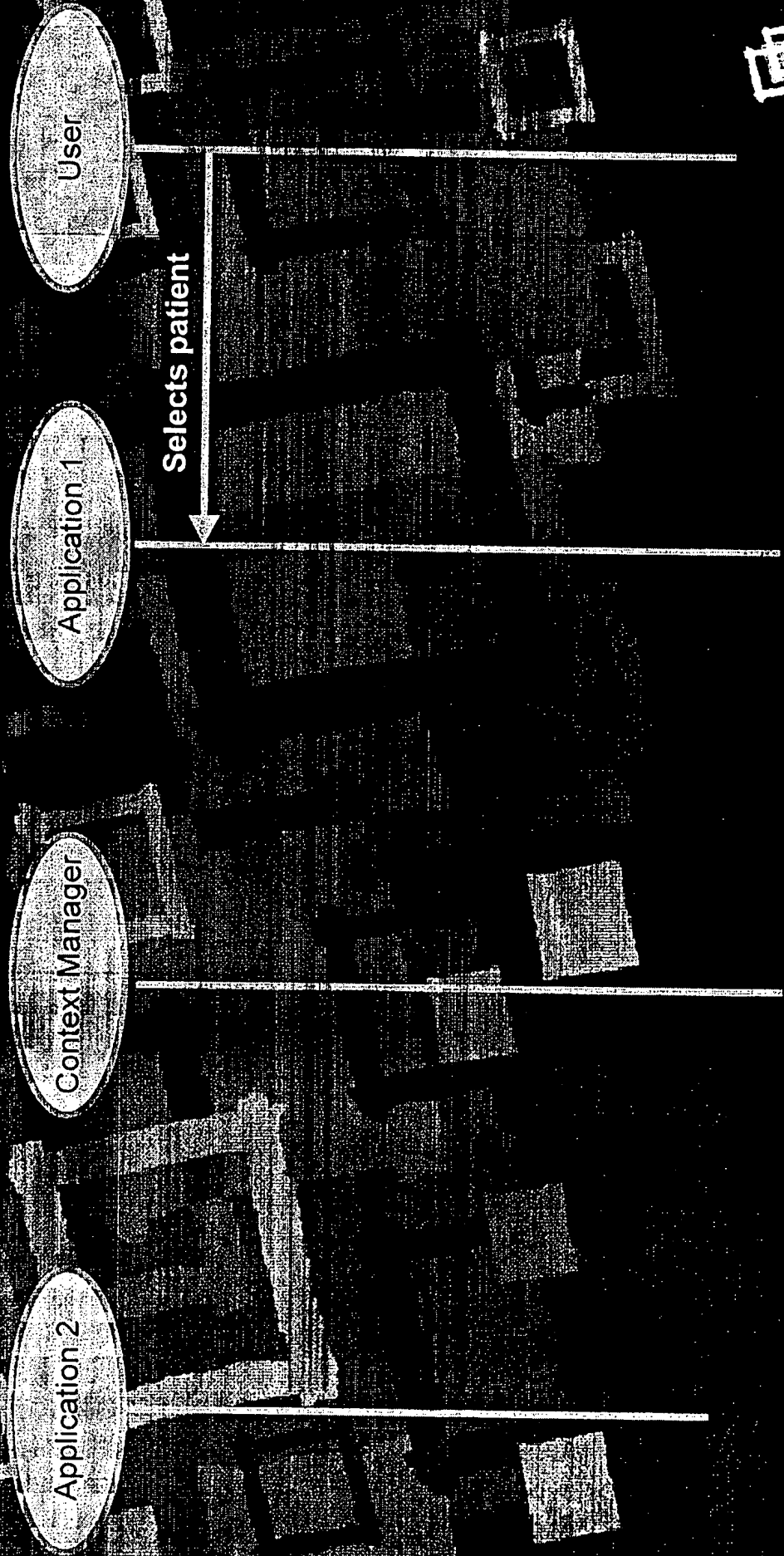


Sentillion
ENABLING INSIGHT

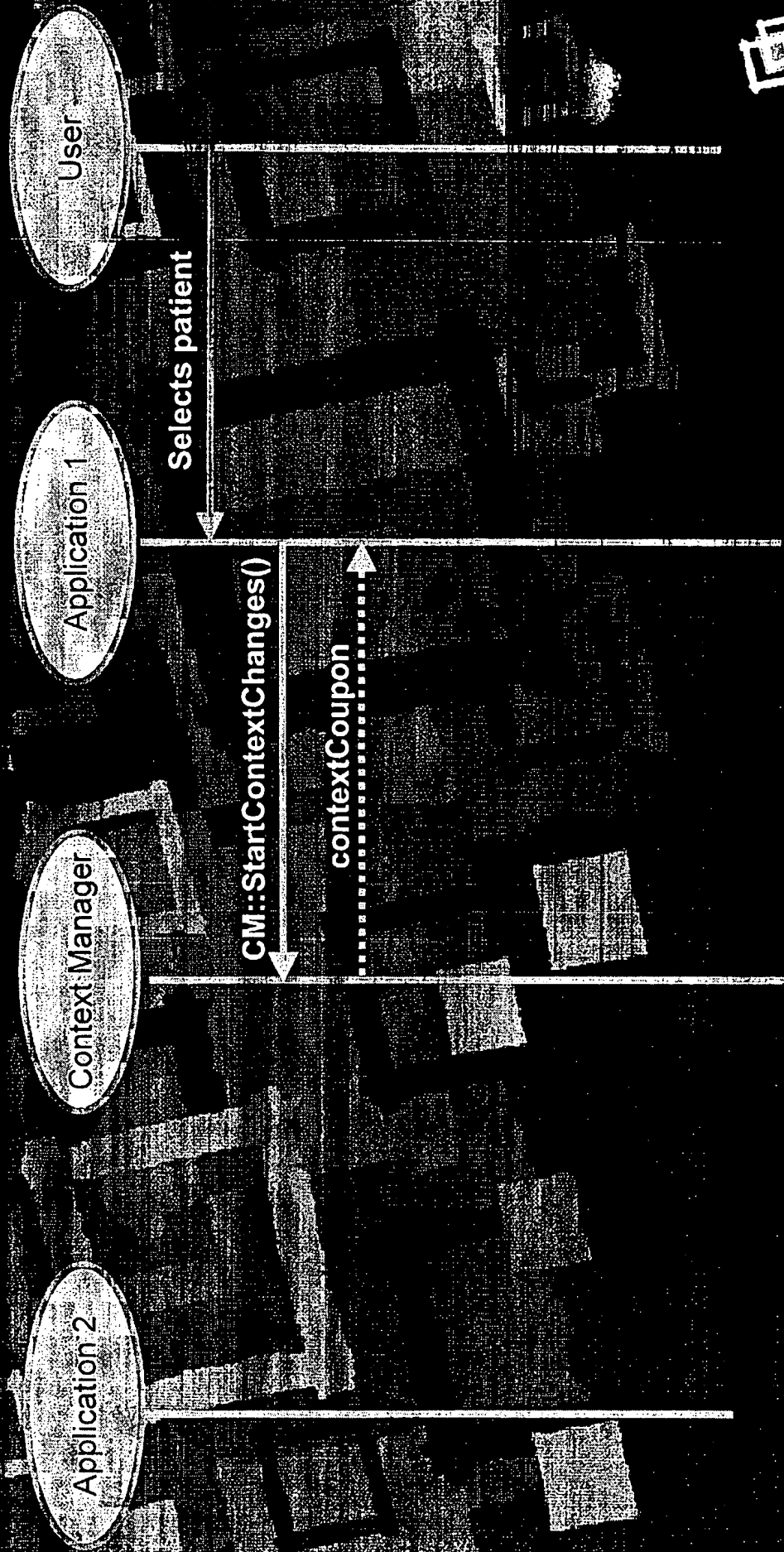
Common Context System: Change Transaction Use Case



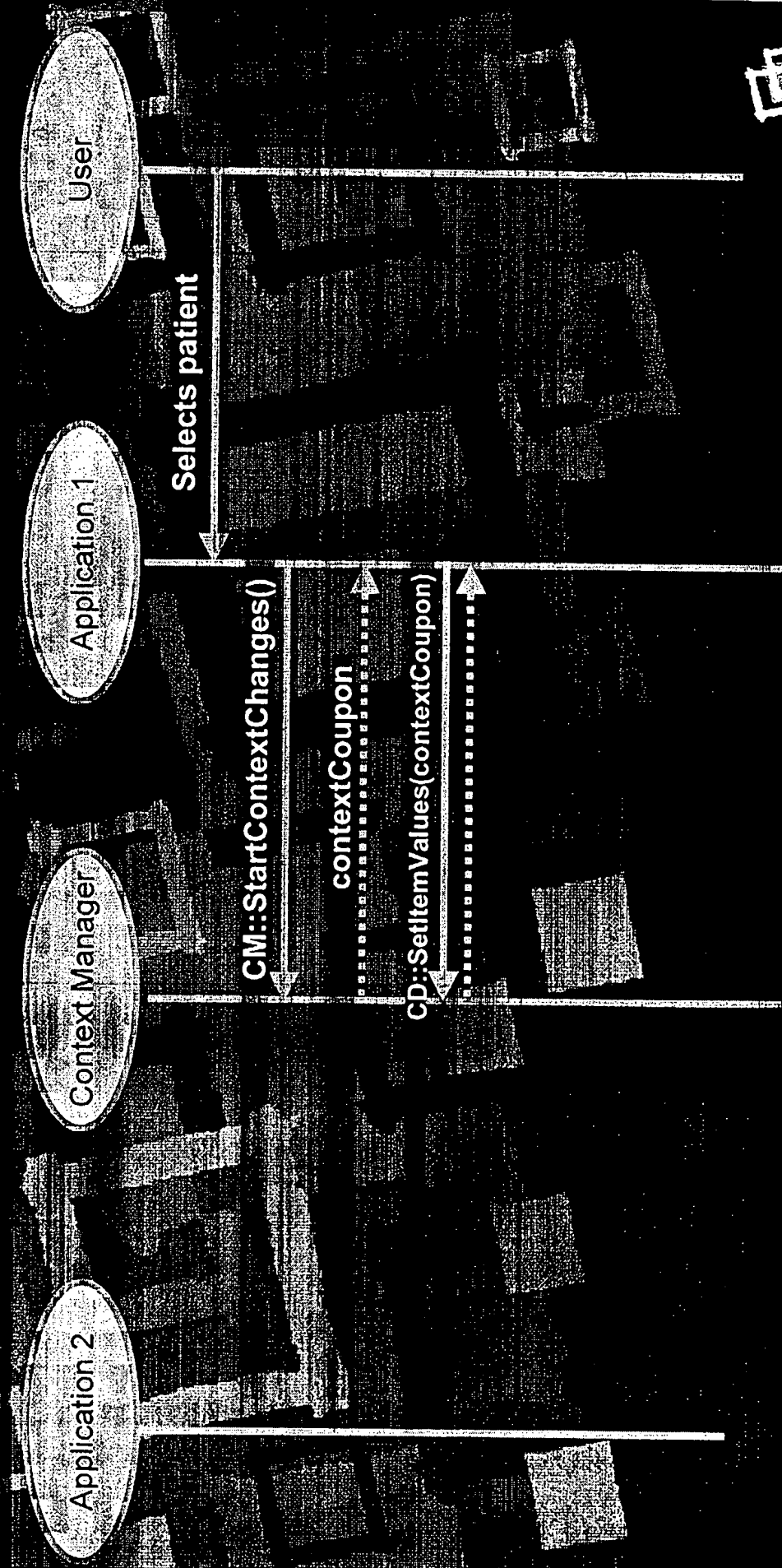
Change Transaction: user sets the context



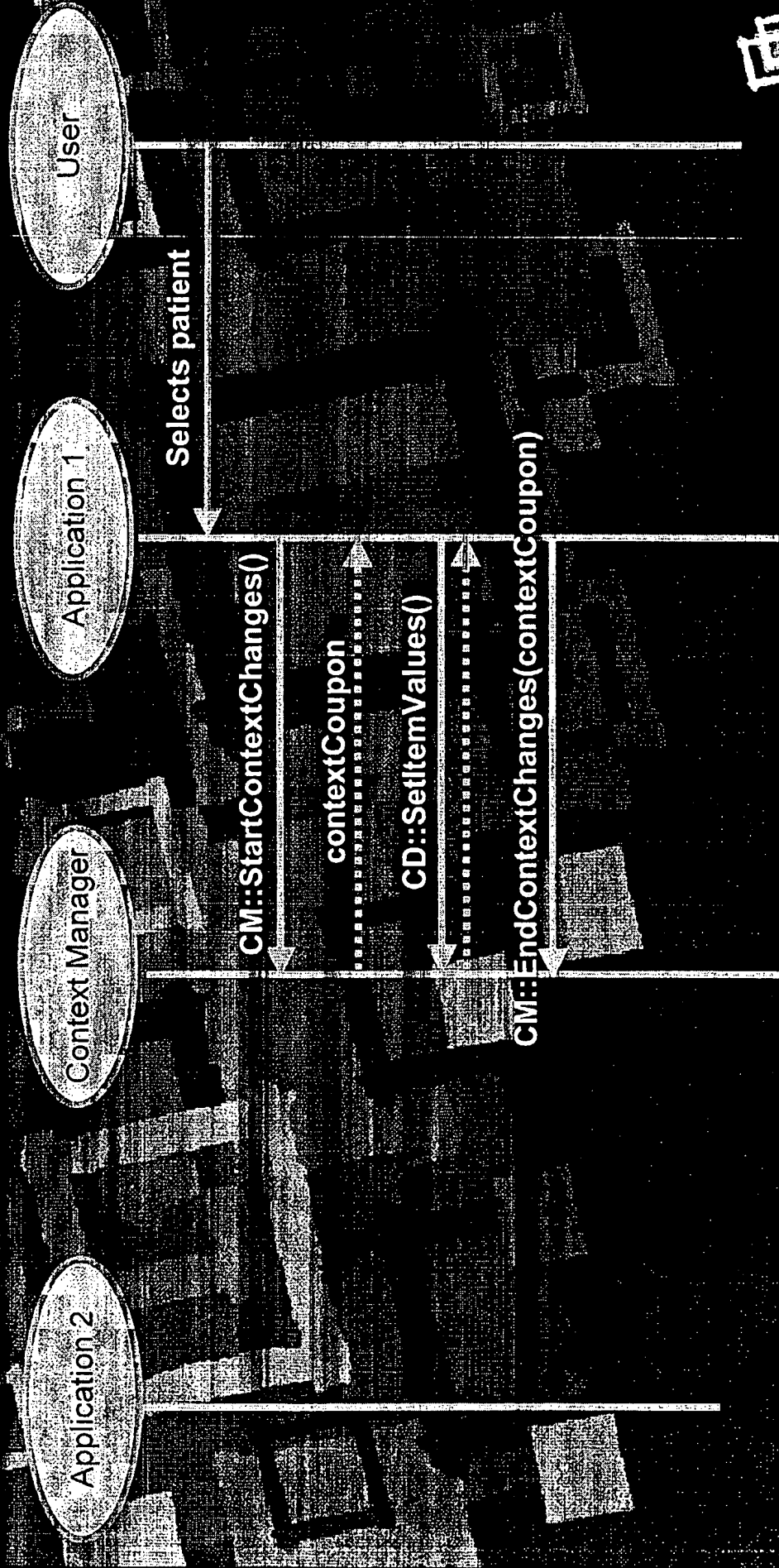
Change Transaction: application starts transaction



Change Transaction: application sets the proposed context

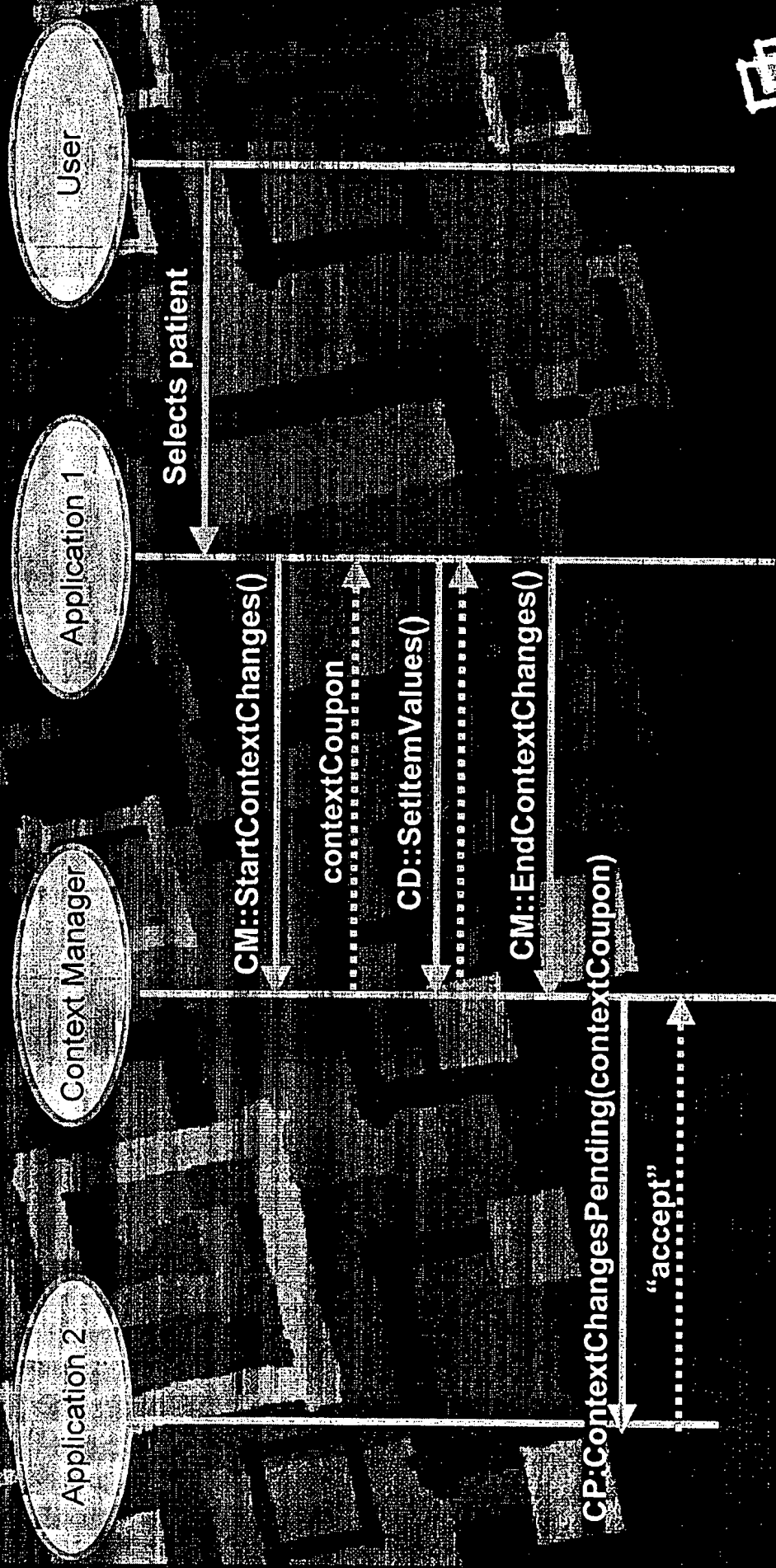


Change Transaction: application finishes its changes

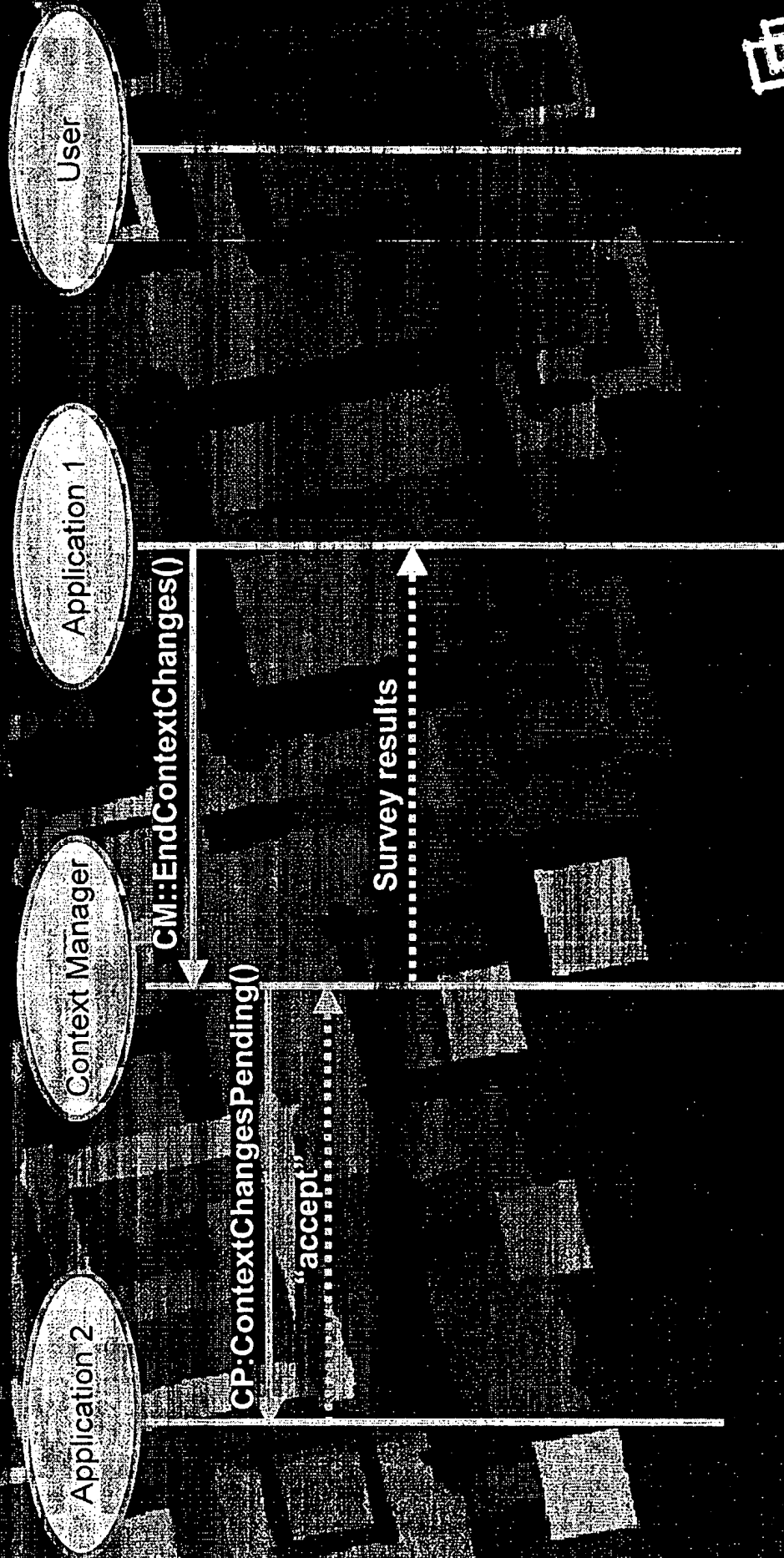


Copyright © 2000 Sentillion, Inc.

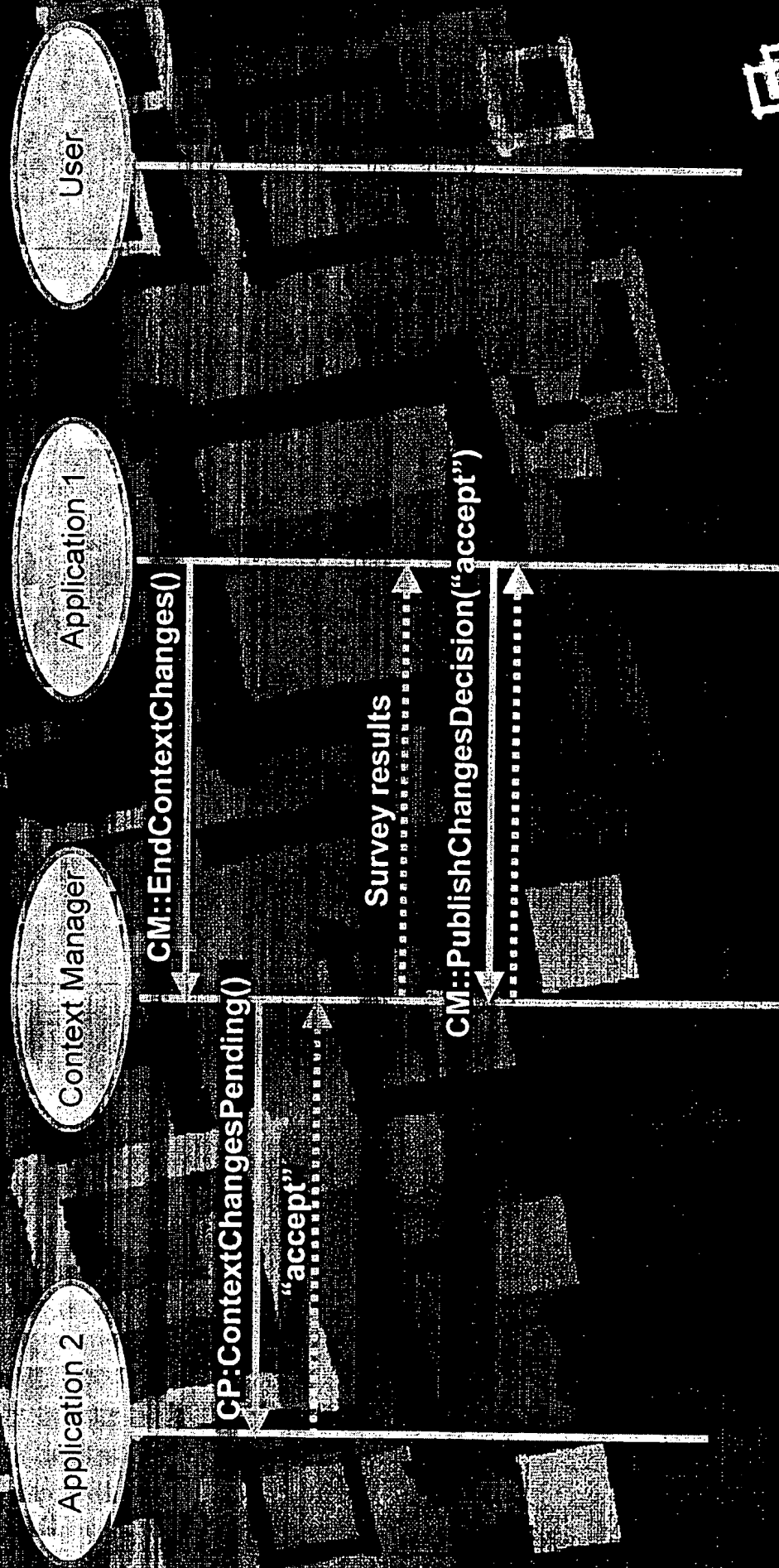
Change Transaction: participants are surveyed --- all accept



Change Transaction: survey results are returned

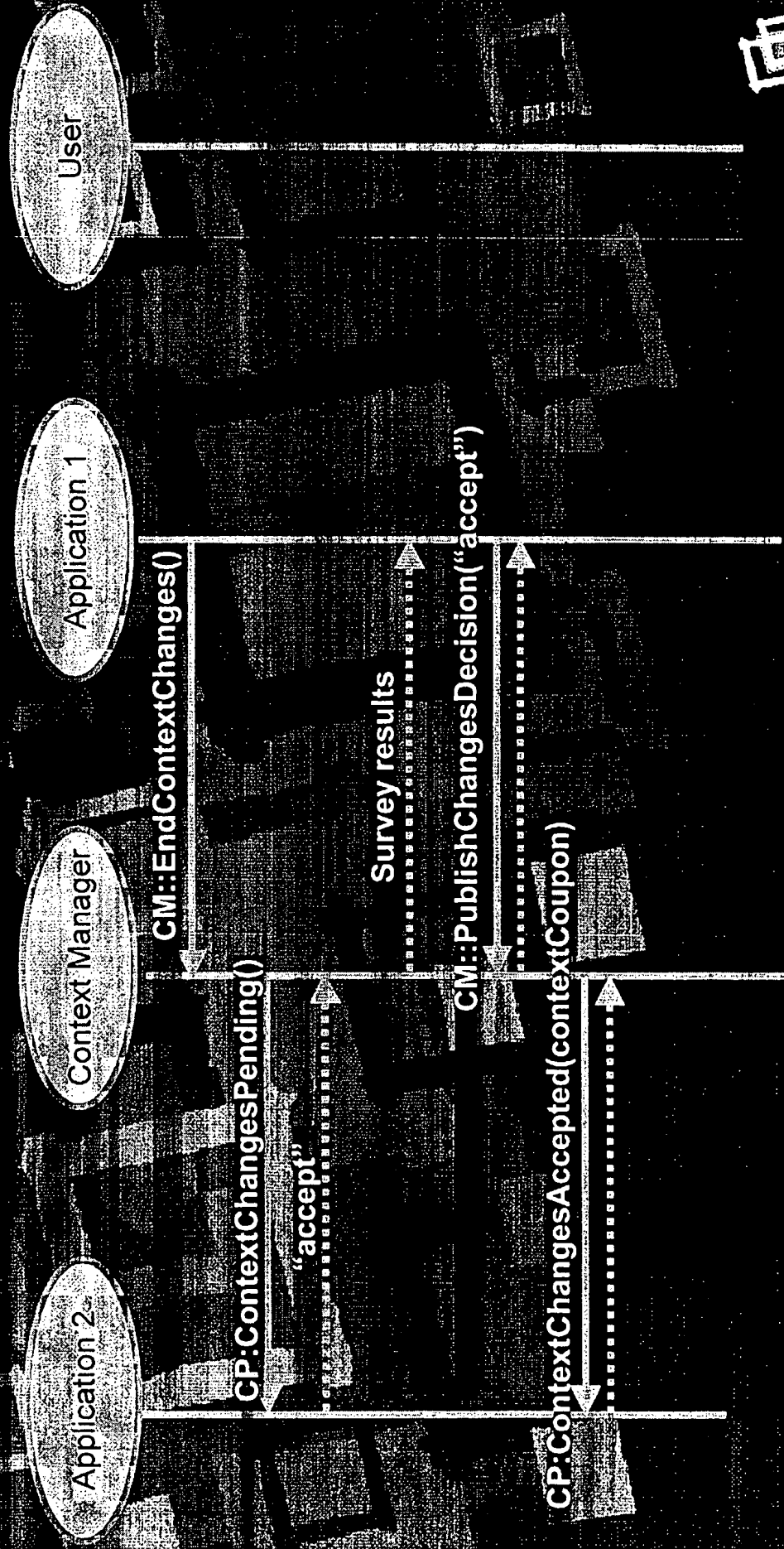


Change Transaction: proposed context is committed

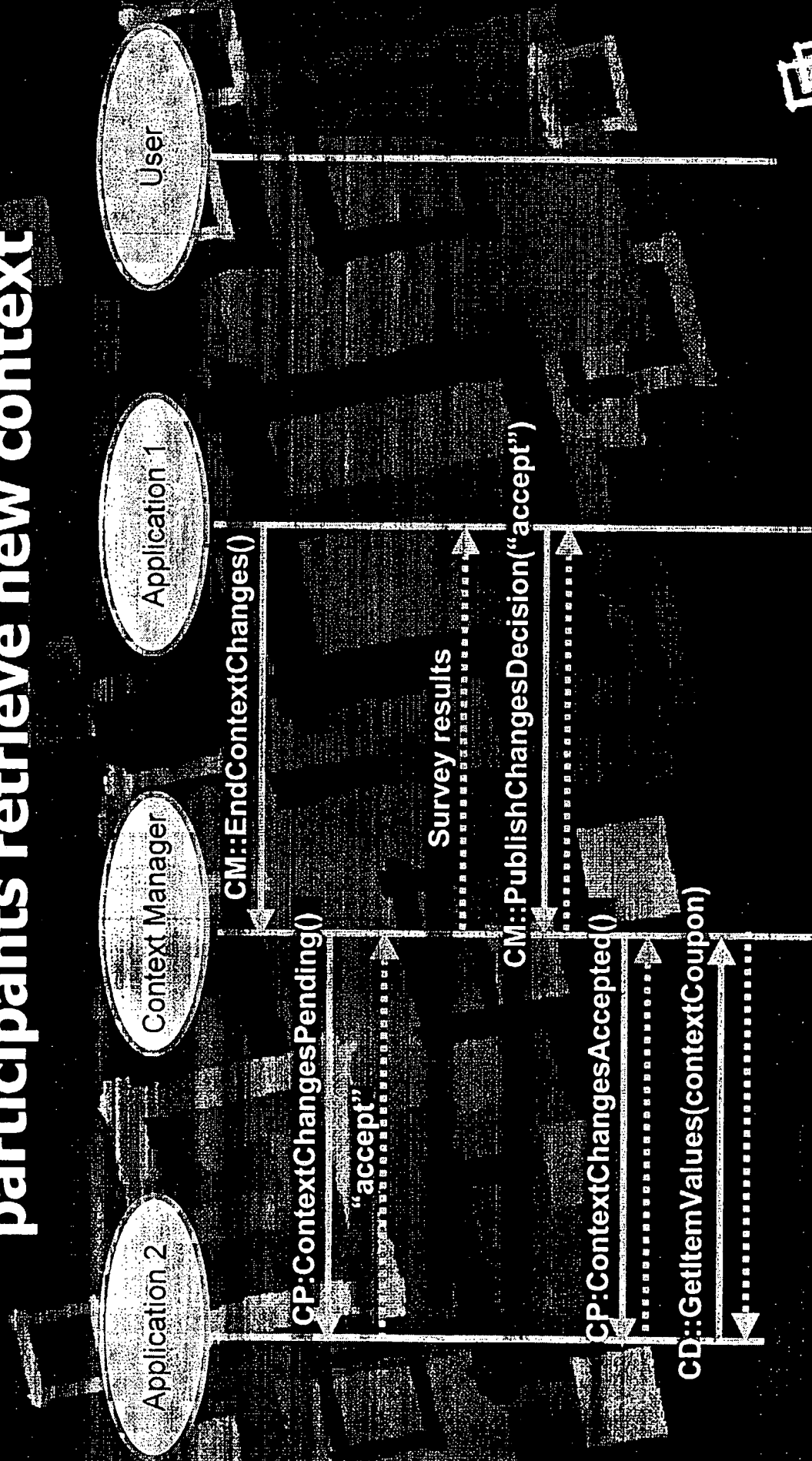


Change Transaction:

participants are notified of acceptance

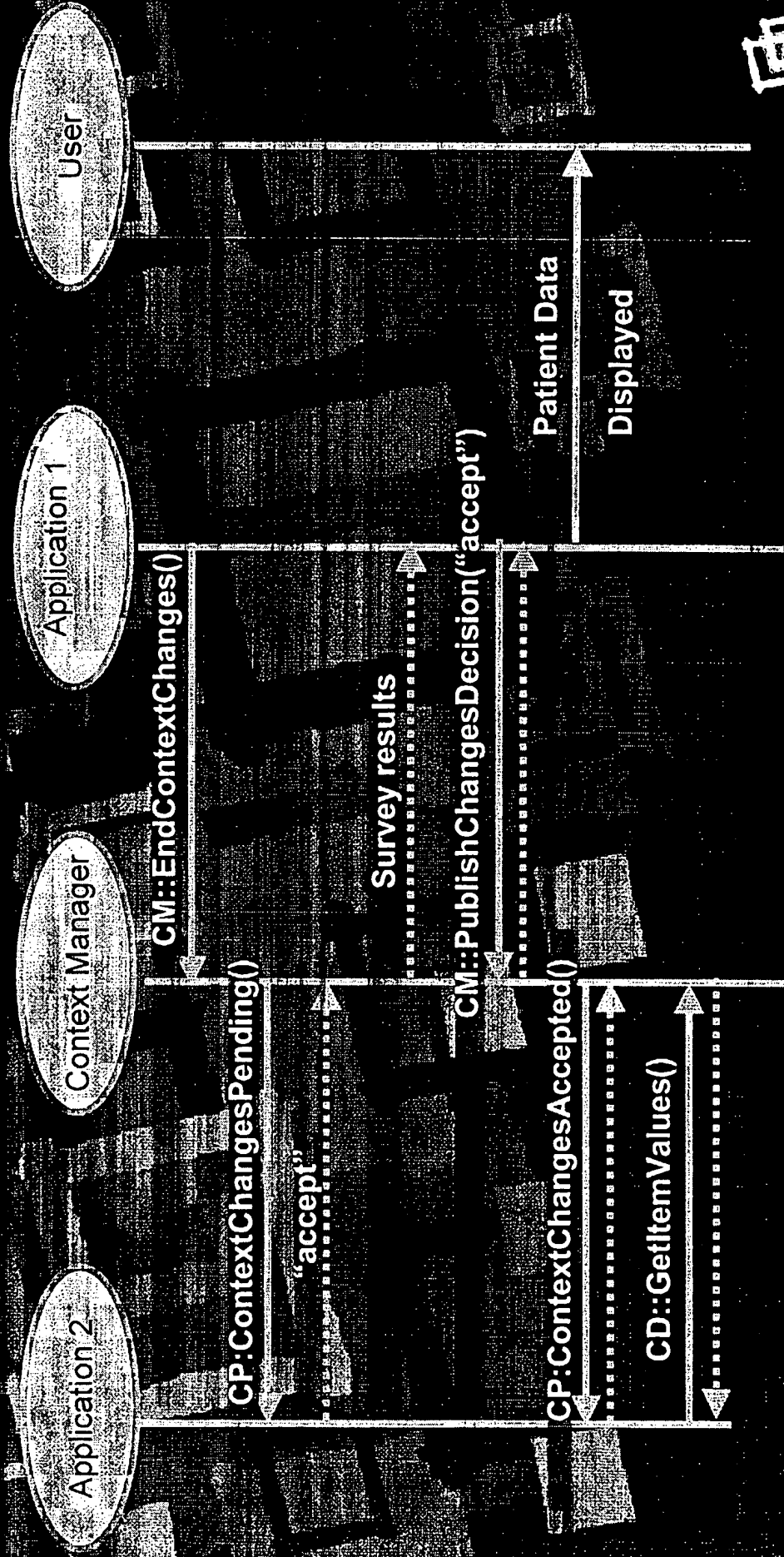


Change Transaction: participants retrieve new context



Change Transaction:

user presented with new patient's data



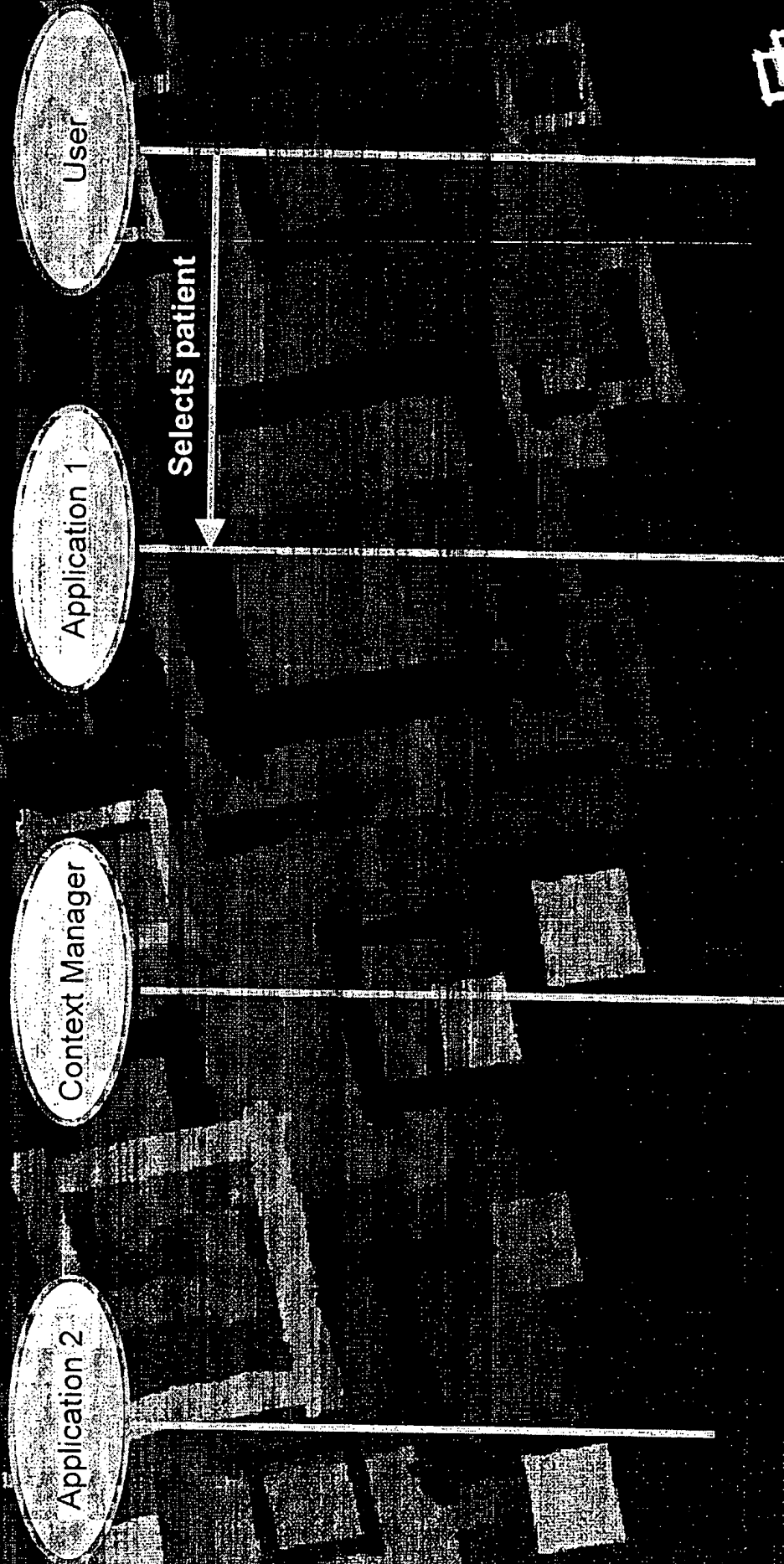
**Wait... There's Another
Possible Ending to the Story!**



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

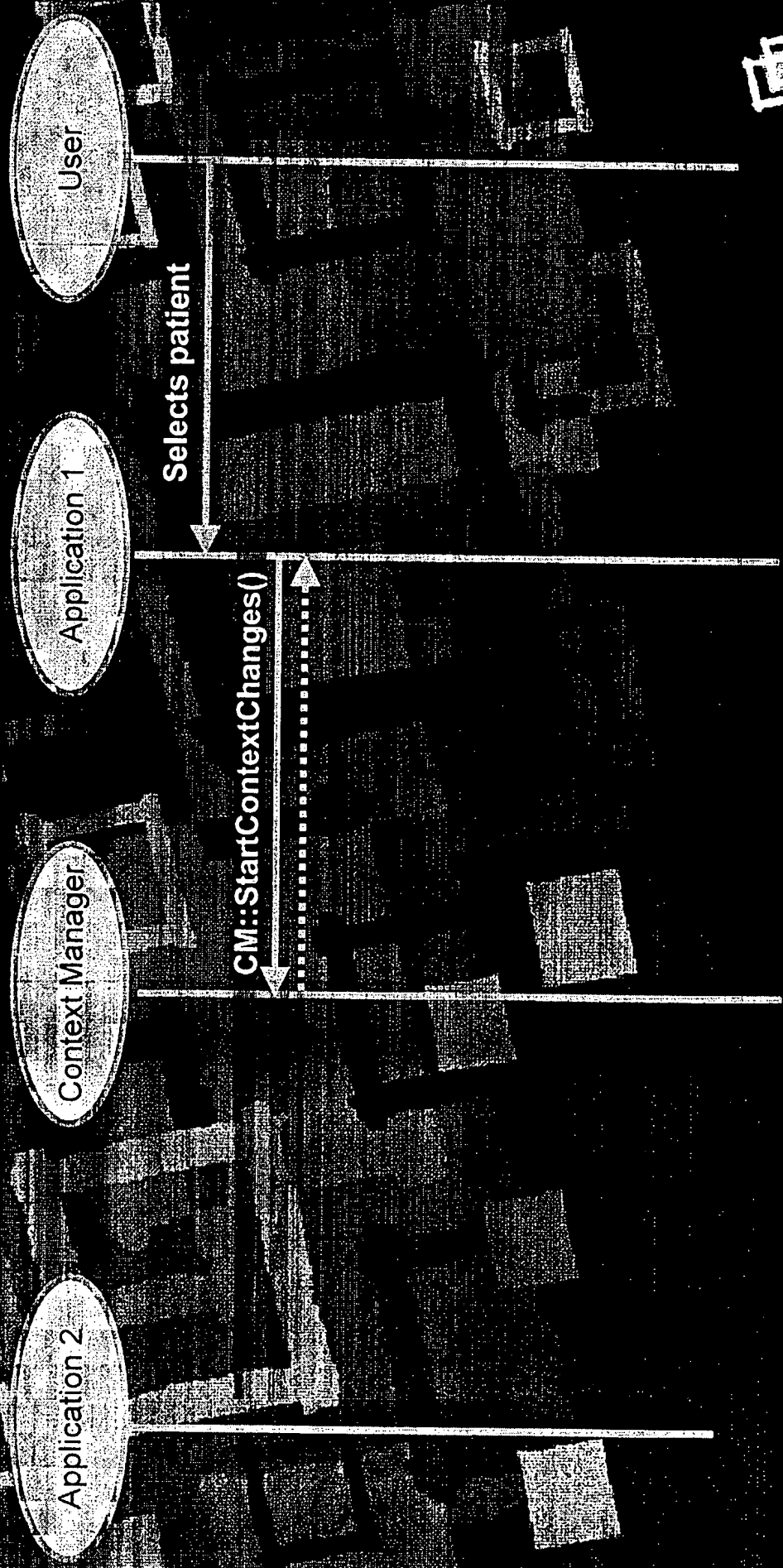
Change Transaction: a survey participant conditionally accepts



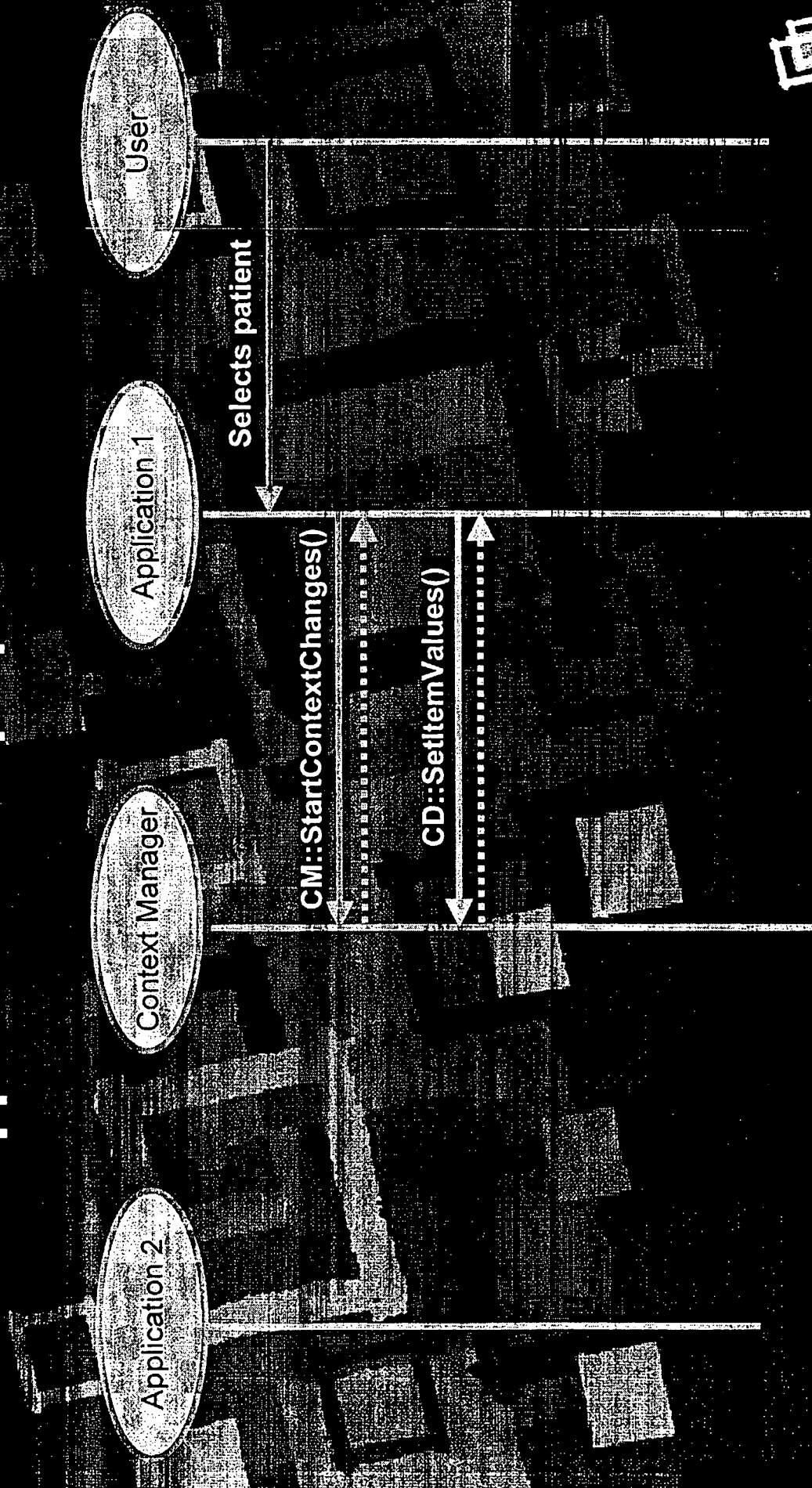
Copyright © 2000 Sentillion, Inc.


Sentillion
ENABLING INSIGHT

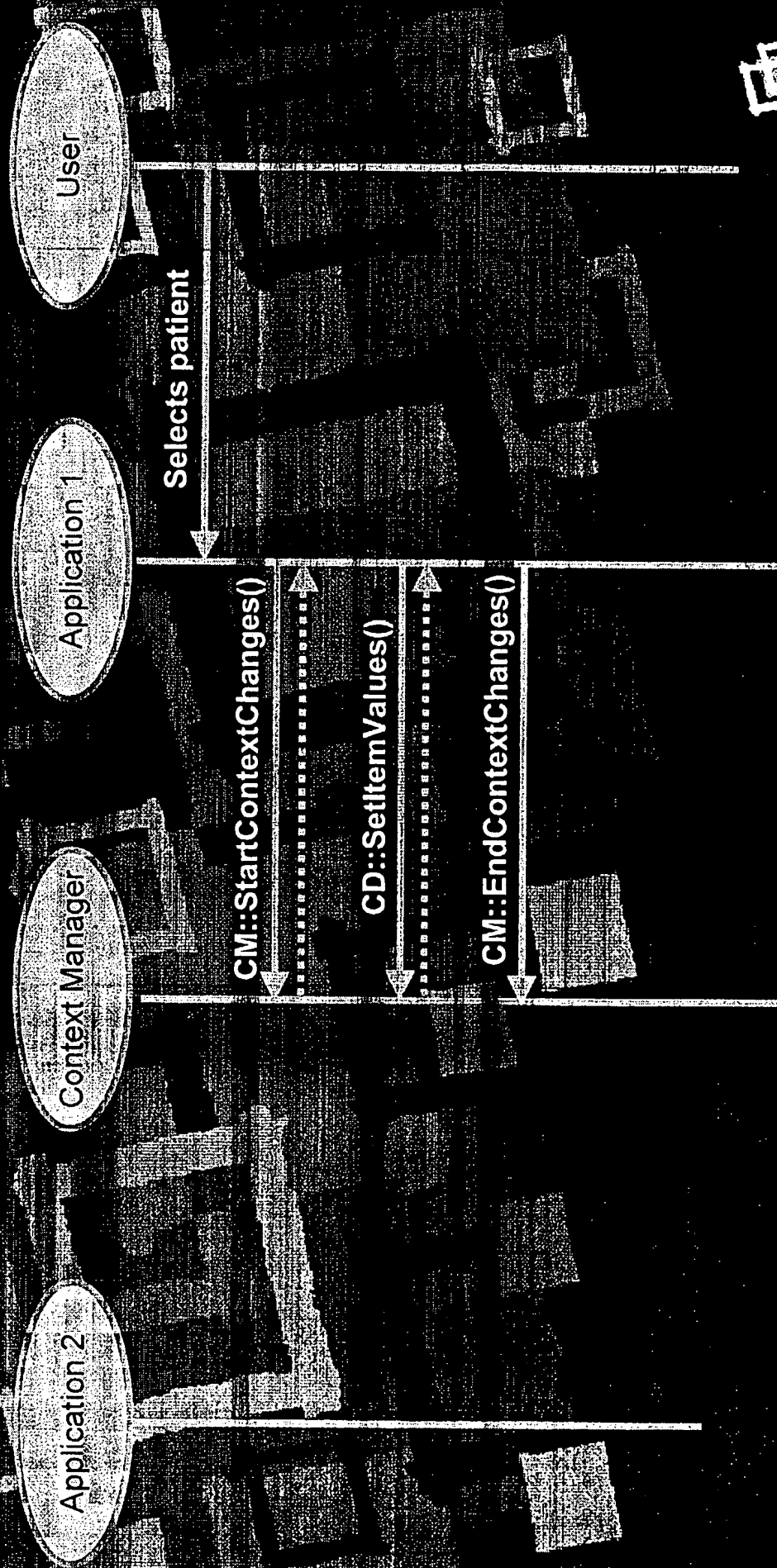
Change Transaction: context transaction started



Change Transaction: application sets proposed context

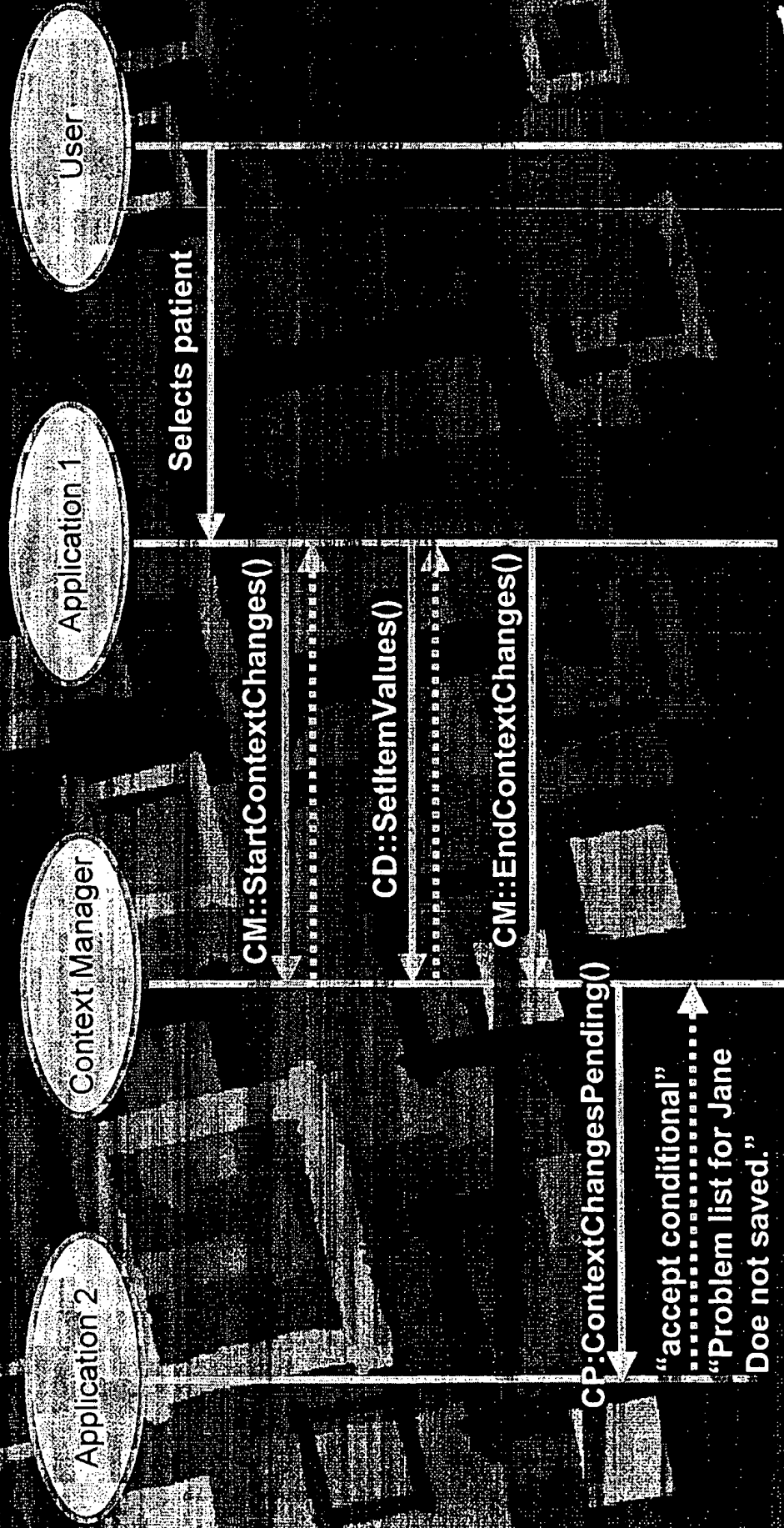


Change Transaction: application finishes setting proposed context

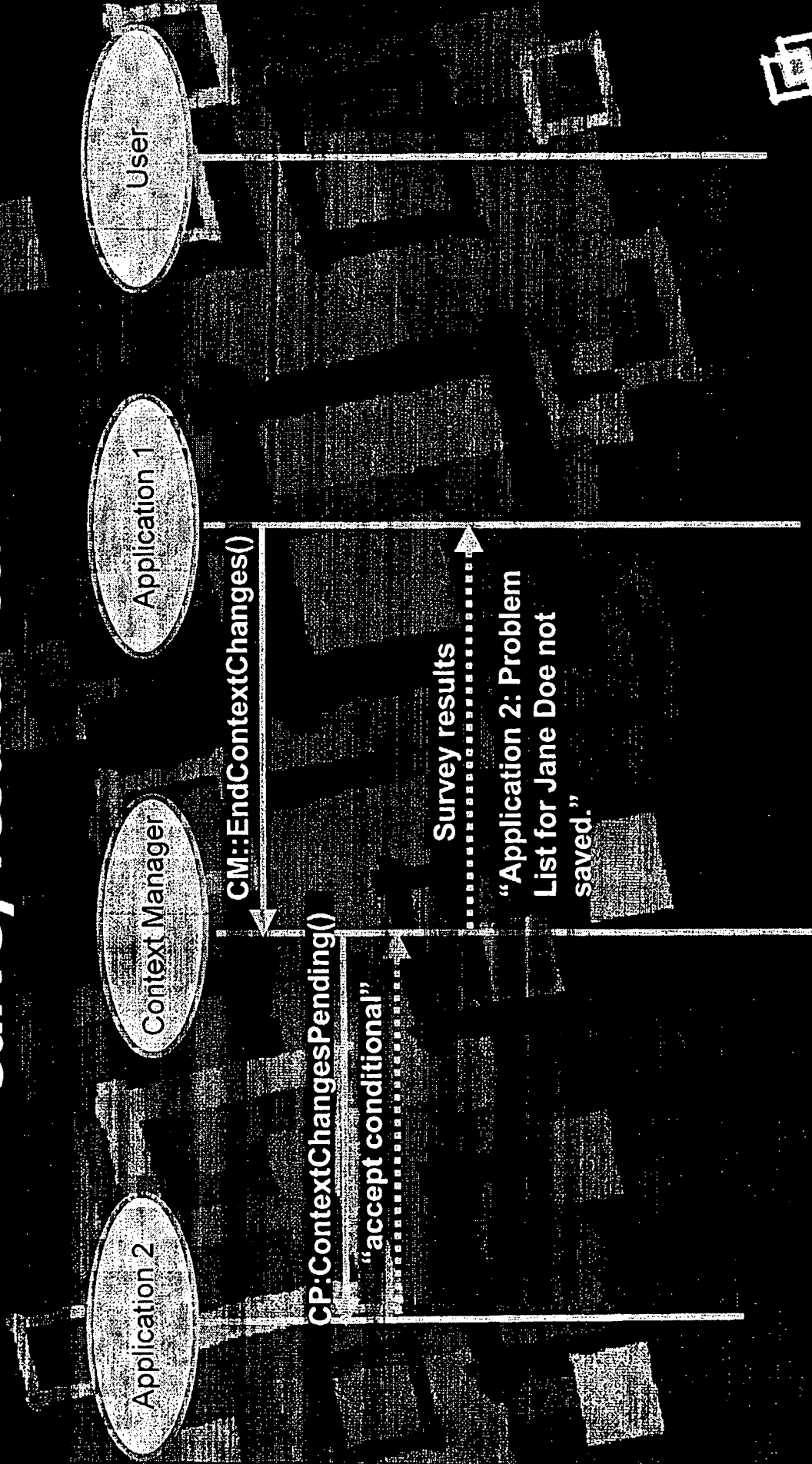


Change Transaction:

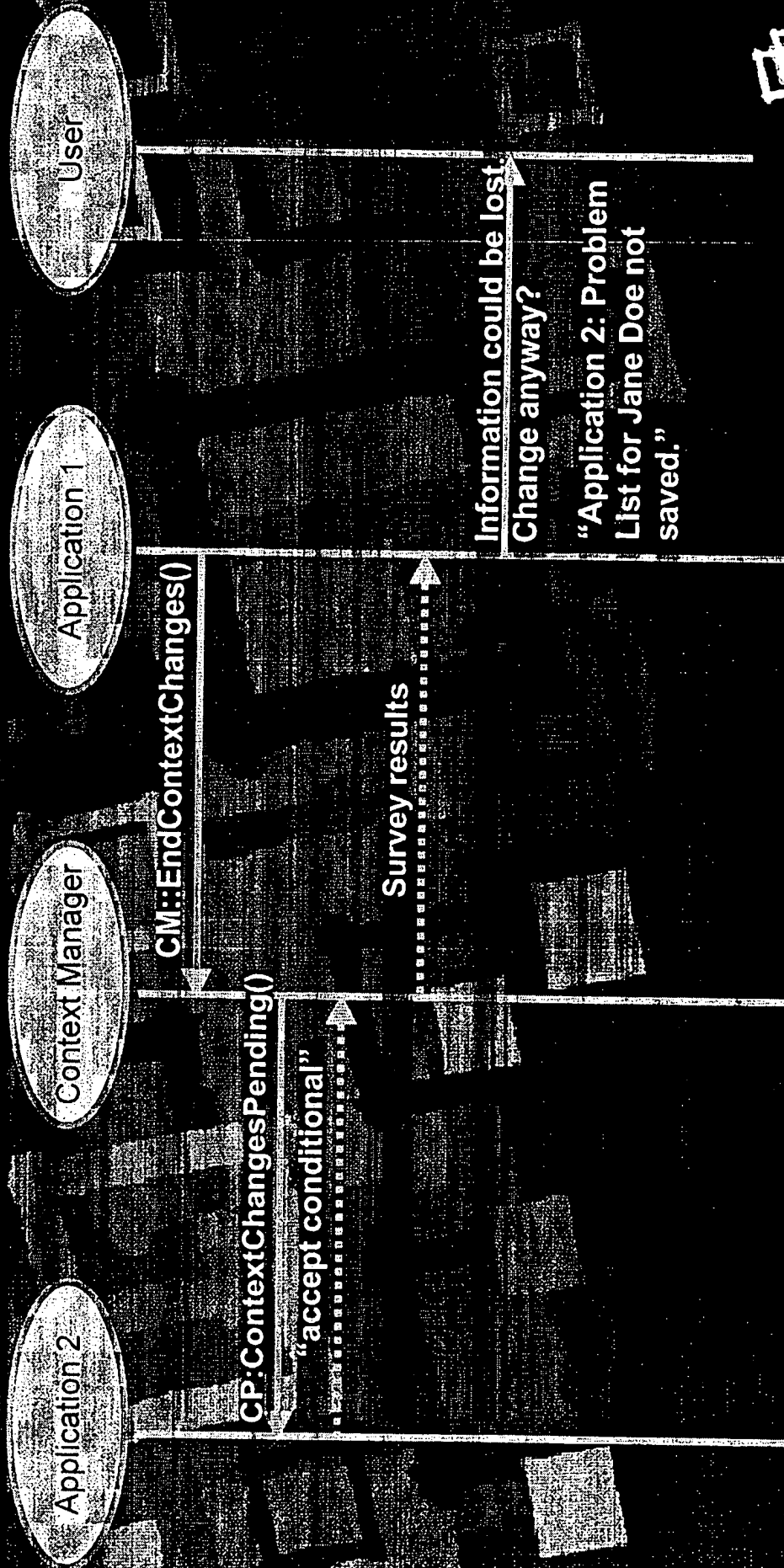
participants are surveyed --- one conditionally
accepts



Change Transaction: survey results returned



Change Transaction: user informed of possible work loss



Recommended Dialog

Problem Changing Clinical Link



There may be a problem changing the current patient. The following application(s) reported a problem. Would you like to continue with the change?

Medical Imaging Application:	Changed data will be lost
EMR Application:	Open patient record will not be saved
Drug Interaction Application:	Prescription will not be send
Diabetes Tracking Application:	Current information will be saved

OK

Cancel

Break link



Sentillion
ENABLING INSIGHT

Clinical Link Icons



Clinical link on



Clinical link broken



Clinical link changing



Sentillion

ENABLING INSIGHT

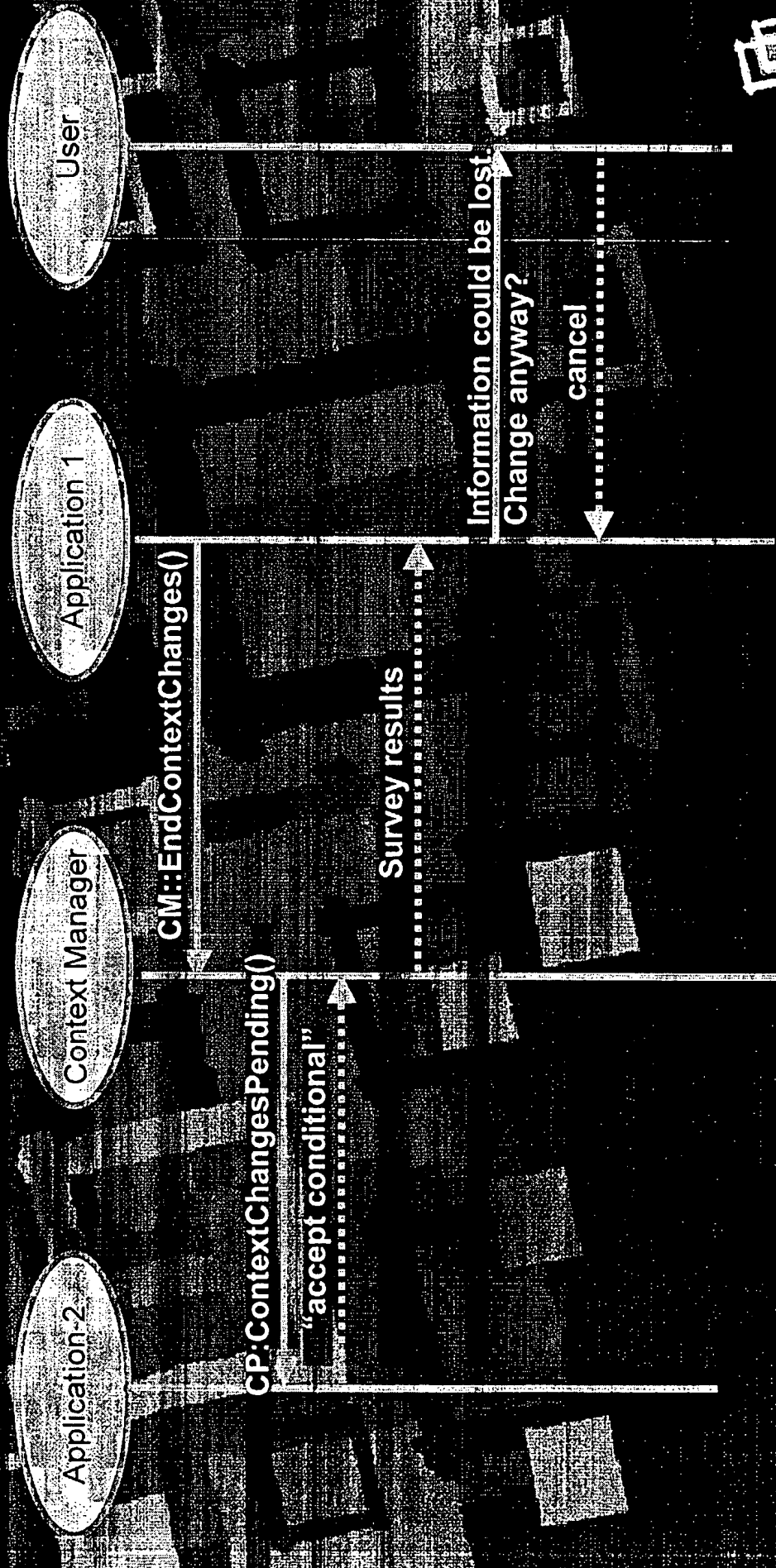
Copyright © 2000 Sentillion, Inc.



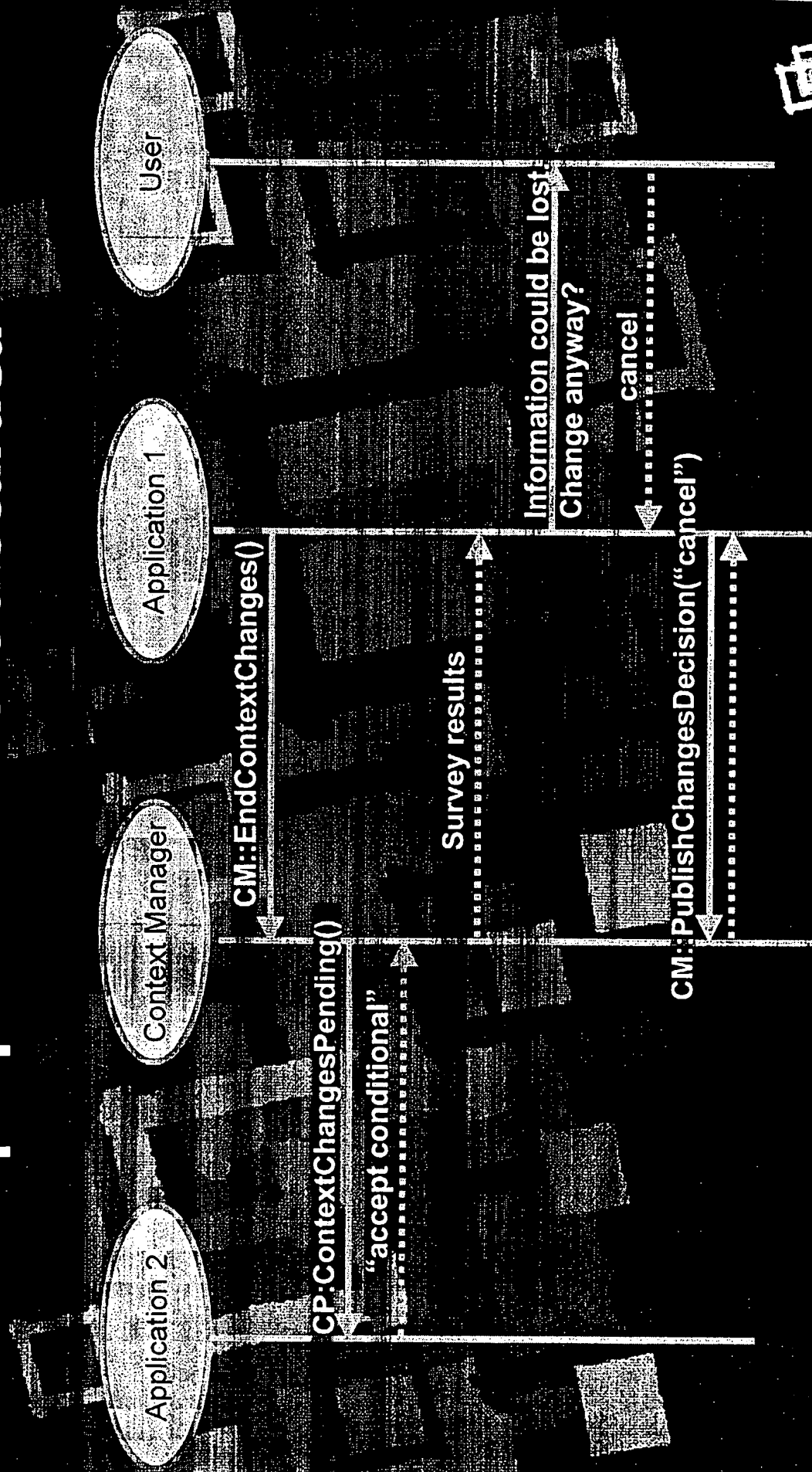

Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

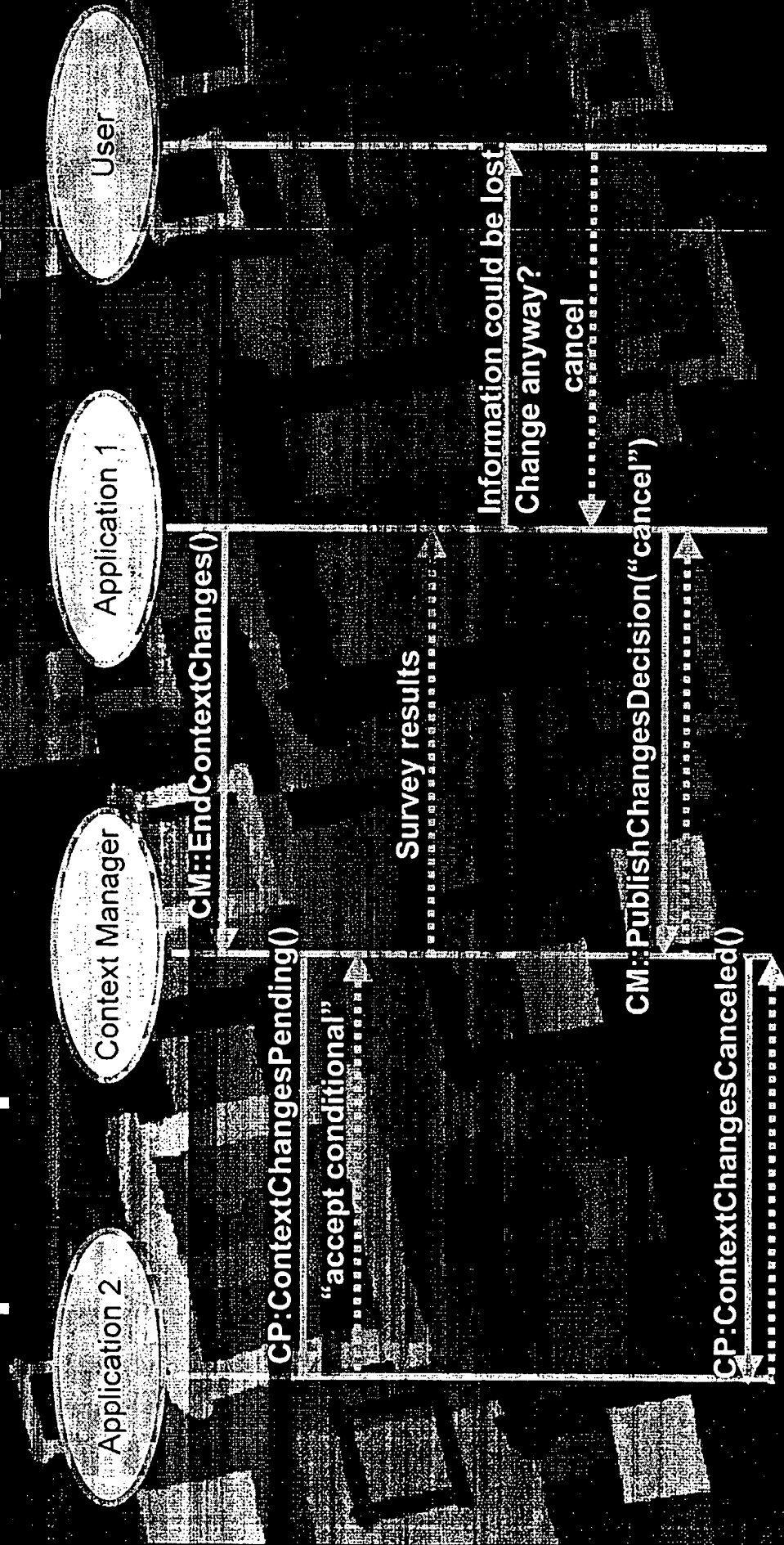
Canceled Change Transaction: user cancels change transaction



Canceled Change Transaction: proposed context discarded



Canceled Change Transaction: participants notified of cancellation



Subtleties

- Must set at least one identifier item, even if value is NULL.
- Applications must have unique labels.
- Once leave the context, assume system is terminated.
- Suspend/resume participation to "step out" without losing slot.
- Mapping agents can only add data.
- Be prepared for user to apply context change anyway.
- It's OK to not offer user a way to cancel changes.



Copyright © 2000 Sentillion, Inc.

 **Sentillion**
ENABLING INSIGHT

ActiveX/COM Mapping

Technology-Neutral

Communication

CCOW IDL

Exceptions

Principal Interface

Interface Interrogation

Interface Registry

Interface Reference

Character Set

Secure Binding Properties

Technology-Specific

COM

Microsoft IDL

HRESULTS

IUnknown

IUnknown::QueryInterface()

Windows Registry

Disp Pointer or Vtbl Pointer

Unicode

CRYPTO32 / RSA / MD5

COM Interface Definitions

Example Interface

```
import "oaidl.idl";
import "ocidl.idl";

[
    object,
    uuid(3E3DD272-998E-11D0-808D-00A0240943E4),
    dual,
    helpstring("IContextParticipant Interface"),
    pointer_default(unique)
]
interface IContextParticipant : IDispatch
{
    [helpstring("informs a participant that a change to the  
common context data is pending")]
    HRESULT ContextChangesPending([in] long contextCoupon,
        [in, out] BSTR* reason,
        [out, retval] BSTR *returnValue);
    // stuff omitted
};
```

COM Exceptions

Example HRESULTS

InvalidContextCoupon

0x80000203L

A context coupon does not match the most recently committed coupon or current transaction coupon

NameValueCountMismatch

0x80000206L

A name array and its corresponding value array do not have the same number of elements.

NotInTransaction

0x80000207L

Attempt to perform a context management transaction when a transaction is not in progress

TransactionInProgress

0x80000209L

Attempt to perform a context management method when a transaction is in progress.

COM Interface Interrogation

```
interface IUnknown{  
    HRESULT QueryInterface(  
        [in] REFIID iid,  
        [out] void ** ppvObject);  
};
```

Lets clients get pointers to other interfaces on a given object.

[in] iid specifies the IID of the interface being requested.

[out] ppvObject receives a pointer to an interface pointer to the object.

Returns S_OK if the interface is supported, S_FALSE if not.



Cryptapi32 Functions

CryptAcquireContext

Acquire a key container (need two)

CryptGenKey

Generate app's key pair within container

CryptExportKey

Export app's public key from container

CryptImportKey

Import context manager's public key

CreateHashObject

Create a new hash object

Do for each
secure
method call

CryptHashData

Compute the hash

CryptGetHashParam

Get the computed hash

CryptDestroyHash

Destroy the hash object

CryptAcquireContext

Release key container (both!)



Sentillion

ENABLING INSIGHT



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

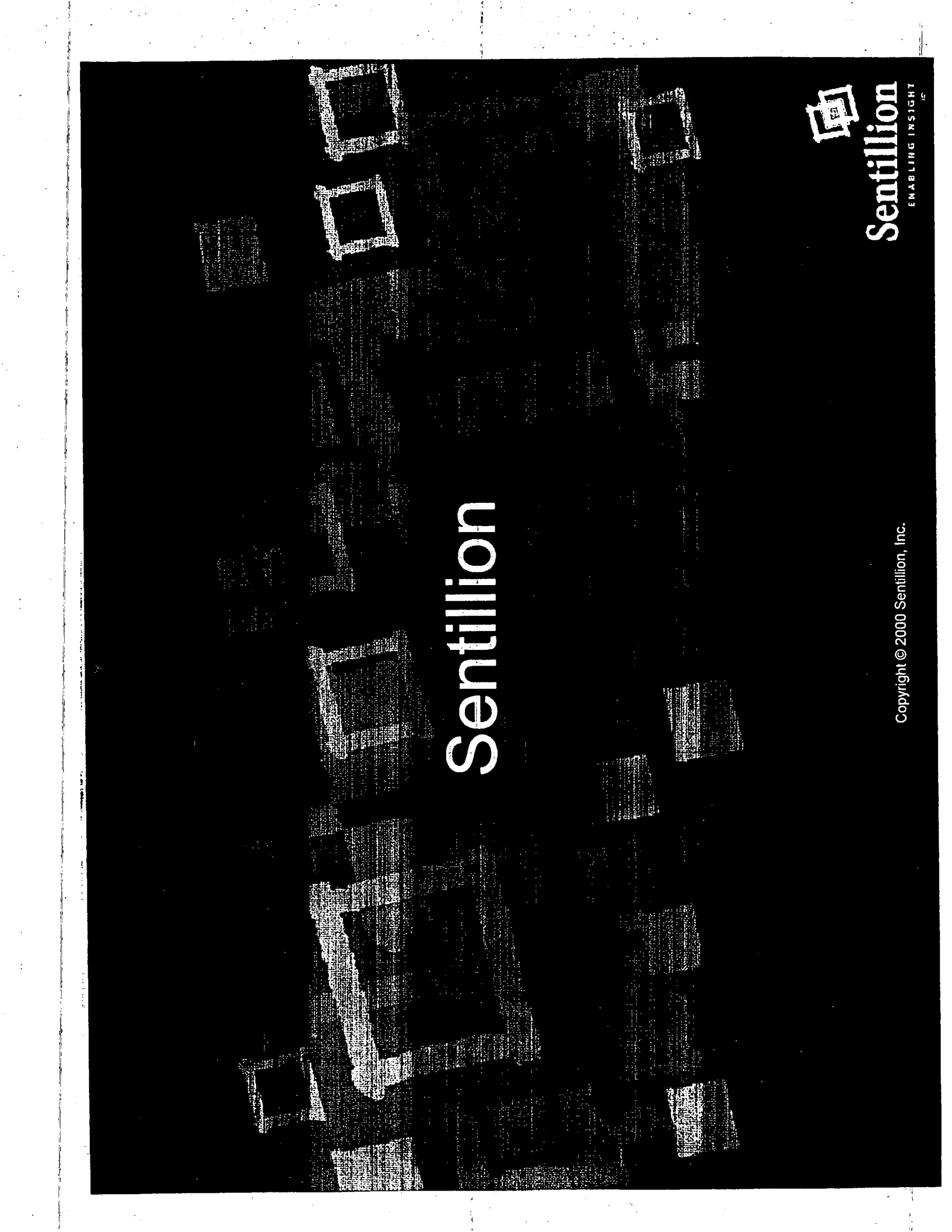
Sentillion's Healthcare Mission



Enable and enhance caregiver
productivity and insight at the
clinical desktop

Copyright © 2000 Sentillion, Inc.





Sentillion

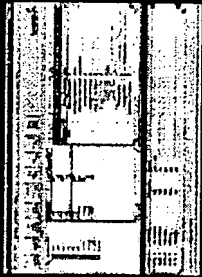


Sentillion

ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Vergence™



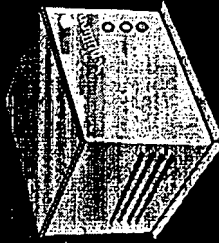
Context
Administrator



Launchpad



- Development Kit
- Validation Kit



Context
Vault



Context
Manager



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Vergence Application SDK

- Enables Windows applications to support CCOW V1.1, including:
 - common links
 - secure links
 - custom links
 - Provides development-time Context Manager and sample applications (incl. source code)
 - Download from www.sentillion.com
- or
- Contact Mary Hall at mhall@sentillion.com
- Now available: SDK for CCOW 1.2 Web applications

Copyright © 2000 Sentillion, Inc.



Sentillion
ENABLING INSIGHT

Terminology Review

Accept, Accept-Conditional	Context participant	Participant coupon
ActiveX	Context subject	Principal interface
Authentication repository	Context item	Private / Public key
Break Link	Corroborating data	RSA
Busy	Digital signature	Secure hash
Chain of trust	Identifier data	Sign-on
Context	Interface	Survey
Component	Interface interrogation	Technology-Neutral
Context Management Arch. (CMA)	Instigator	Use case
Component Object Model (COM)	Mapping agent	User Link
Context change coupon	Msg Authentication Code	W3C
Context change transaction	Patient Link	
Context manager	Passcode	

More Information

- www.hl7.org (Technical Committees)
- [Sentillion, info@sentillion.com](mailto:info@sentillion.com)
- www.sentillion.com

Copyright © 2000 Sentillion, Inc.



Sentillion
ENABLING INSIGHT

About Us

Standards
Leadership

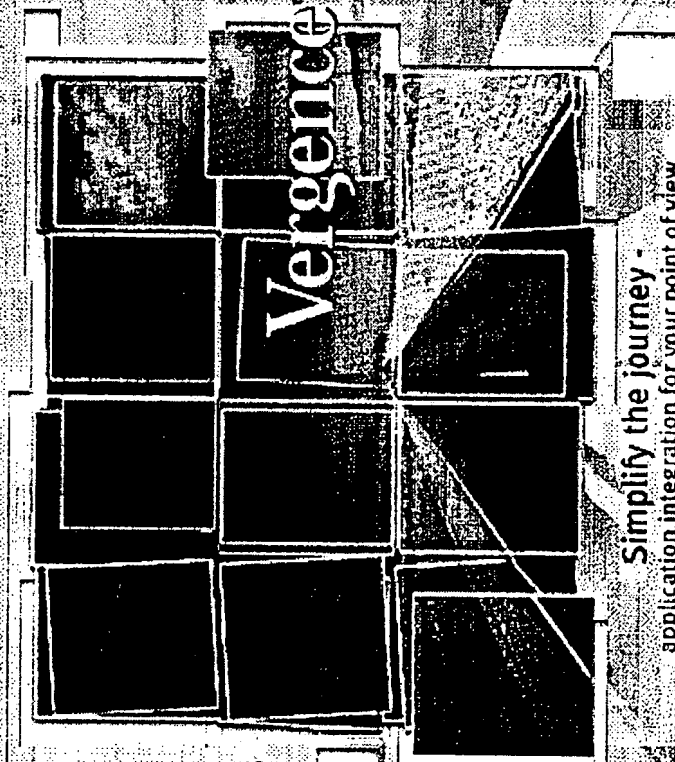
Adaptive
Model

Partnerships

Training
& Support

Consulting
Services

Marketing
Assistance



Simplify the journey -
application integration for your point of view

Designed for Healthcare

Enable Institution's Ownership

Industry Leadership

Flexible Business Model

Innovative and Practical

Platform for Now and Future

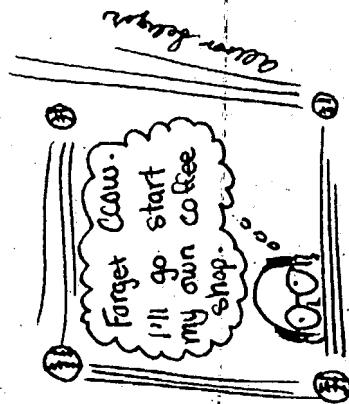
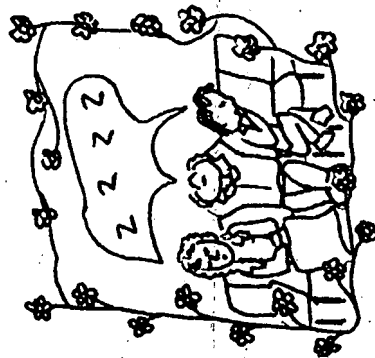
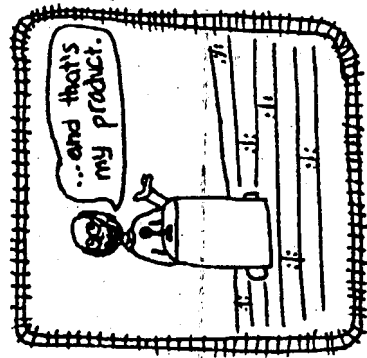
Products Shipping Now



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Something
New...
by Alison
Seliger





Sentillion

ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

COM Interface Interrogation

C++:

Explicit use of `IUnknown::QueryInterface`.

VisualBasic:

Implicit.

J++:

Java-style cast.



Sentillion
ENABLING INSIGHT

Windows Registry

Component

Prog Id

Context Manager

CCOW.ContextManager

Patient Mapping Agent

CCOW.MappingAgent_Patient

User Mapping Agent

CCOW.MappingAgent_User

Context Participant App

None needed



COM Example

Join Common Context

```
// C++
#import "Program Files\Sentillion\ContextManager\ContextManager.tlb"
CONTEXTMANAGERLib::IContextManagerPtr iCM;
iCM.CreateInstance(L"CCOW.ContextManager.1");
long myCoupon = iCM->JoinCommonContext(myLabel, ...);
```

```
// VisualBasic®
ContextManagerObj As Object New ContextManager
iCM As IContextManager
Set ContextManagerObj = CreateObject("CCOW.ContextManager.1")
Set iCM = ContextManagerObj
Dim myCoupon As Long
myCoupon = iCM.JoinCommonContext(myLabel, ...);
```

```
// J++
import CCOW.ContextManager.*;
IContextManager iCM = (IContextManager) new ContextManager();
long myCoupon = iCM.JoinCommonContext(myLabel, ...);
```



Sentillion
ENABLING INSIGHT

COM Example

Set The Context

```
// C++  
long contextCoupon = iCM->StartContextChanges(...);  
VARIANT names = // names of items to set  
VARIANT values = // values of items to set  
iCD->SetItemValues(participantCoupon, names, values, contextCoupon);  
VARIANT vote = iCM->EndContextChanges(contextCoupon, ...);  
BSTR decision = // Decide how to proceed -- ask user if necessary  
iCM->PublishChangesDecision(contextCoupon, decision);
```

COM Example

Get The Context

```
// C++  
VARIANT names = iCD->GetItemNames();  
VARIANT values = iCD->GetItemValues(names, contextCoupon, ...);
```



Sentillion
ENABLING INSIGHT

Web Mapping

Technology-Neutral

Communication

CCOW IDL

Exceptions

Principal Interface

Interface Interrogation

Interface Registry

Interface Reference

Character Set

Secure Binding Properties

Technology-Specific

HTTP w/URL Encoding

Encoded URL Definitions

Encoded in HTTP Reply Msg

Interface Information

Interrogate()

Context Management Registry

URL

US-ASCII + ASCII-Encoded Unicode

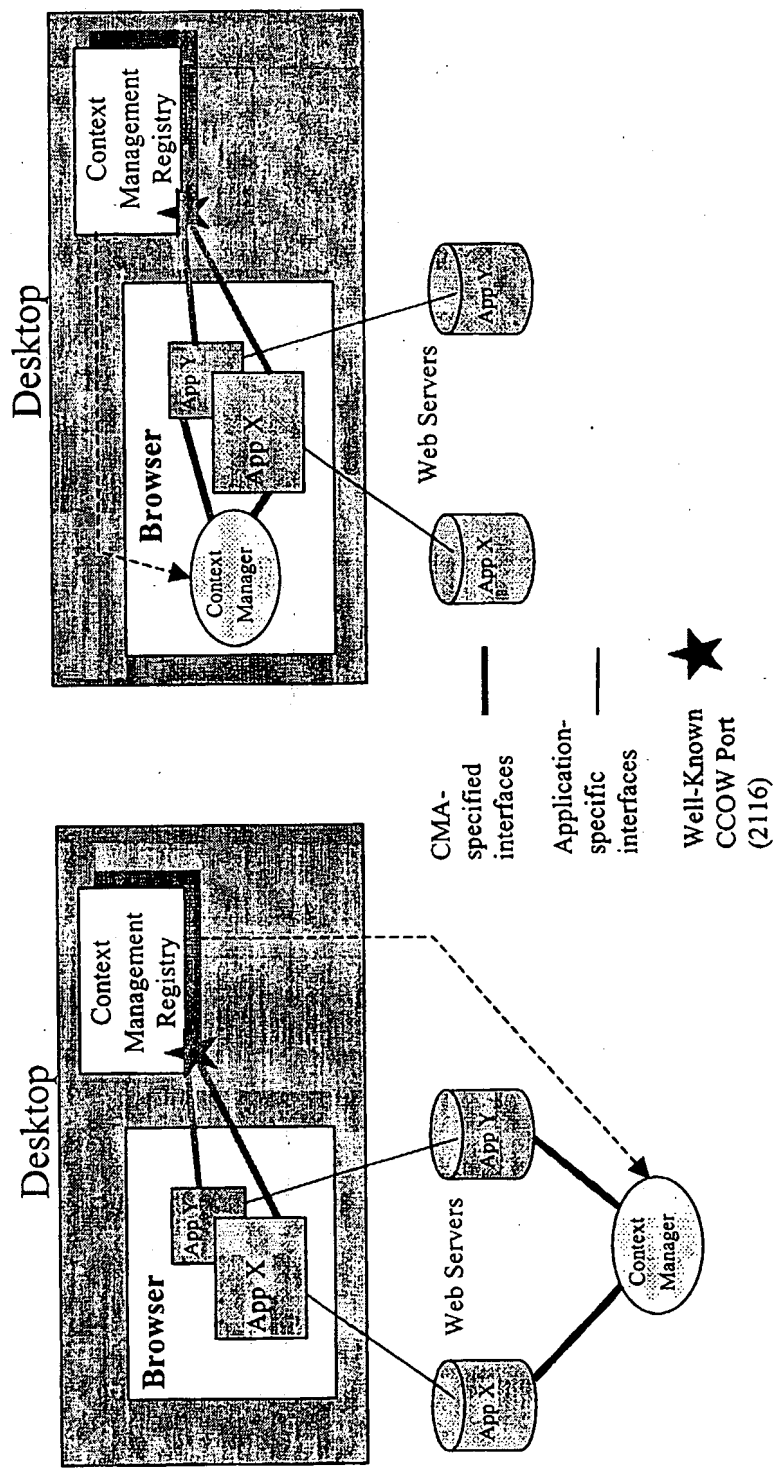
Web / RSA / MD5

Copyright © 2000 Sentillion, Inc.



Sentillion
ENABLING INSIGHT

Web Component Distribution



Client Centric Solution

Server Centric Solution

HTTP Interface Definitions

Example Interface

HTTP Request Message

Argument Name	Data Type	Comment
interface	string	"ContextManager"
method	string	"StartContextChanges"
participantCoupon	long	
HTTP Reply Message		
contextCoupon	long	

HTTP Request Message

Argument Name	Data Type	Comment
interface	string	"ContextManager"
method	string	"EndContextChanges"
contextCoupon	long	
HTTP Reply Message		
noContinue	boolean	
responses	string[]	

Etc....

Copyright © 2000 Sentillion, Inc.

Encoded URL

Example

<http://www.mcis.duke.edu/ccow/contextManager?>

[&interface=ContextManager](http://www.mcis.duke.edu/ccow/contextManager?&interface=ContextManager)

[&method=SetItemValues](http://www.mcis.duke.edu/ccow/contextManager?&method=SetItemValues)

[&itemNames=Patient.Id.MRN.icu|Patient.Co.Name](http://www.mcis.duke.edu/ccow/contextManager?&itemNames=Patient.Id.MRN.icu|Patient.Co.Name)

[&itemValues=123-813-JMDH-79|Marchant^Kyle^^^^](http://www.mcis.duke.edu/ccow/contextManager?&itemValues=123-813-JMDH-79|Marchant^Kyle^^^^)

[&contextCoupon=27](http://www.mcis.duke.edu/ccow/contextManager?&contextCoupon=27)

[&appSignature=0BC12D890913E9C1D00BB9832A81238](http://www.mcis.duke.edu/ccow/contextManager?&appSignature=0BC12D890913E9C1D00BB9832A81238)

HTTP Exceptions

Example Exception Messages

exception=InvalidContextCoupon

A context coupon does not match the most recently committed coupon or current transaction coupon

exception=NameValueCountMismatch

A name array and its corresponding value array do not have the same number of elements.

exception=NotInTransaction

Attempt to perform a context management transaction when a transaction is not in progress

exception=TransactionInProgress

Attempt to perform a context management method when a transaction is in progress.



HTTP Interface Interrogation

HTTP Request Message

Argument Name	Data Type	Comment
interface	string	"InterfaceInformation"
method	string	"Interrogate"
interface	string	The name of the interface of interest. Case Sensitive.

HTTP Reply Message

implemented	boolean	True if implemented, false otherwise.
-------------	---------	---------------------------------------

Context Management Registry

HTTP Request Message		
Argument Name	Data Type	Comment
interface	string	"ContextManagementRegistry"
method	string	"Locate"
componentName	string	The name of the component to locate.
version	string	The CMA version of the desired component
descriptiveData	string	Additional data used to describe the component of interest. The allowed values and interpretation of this parameter depends upon the type of component (see below).
HTTP Reply Message		
componentUrl	string	The URL of the desired component.

componentName="CCOW.ContextManager"

version = "1.2"

descriptiveData= not currently used

Copyright © 2000 Sentillion, Inc.

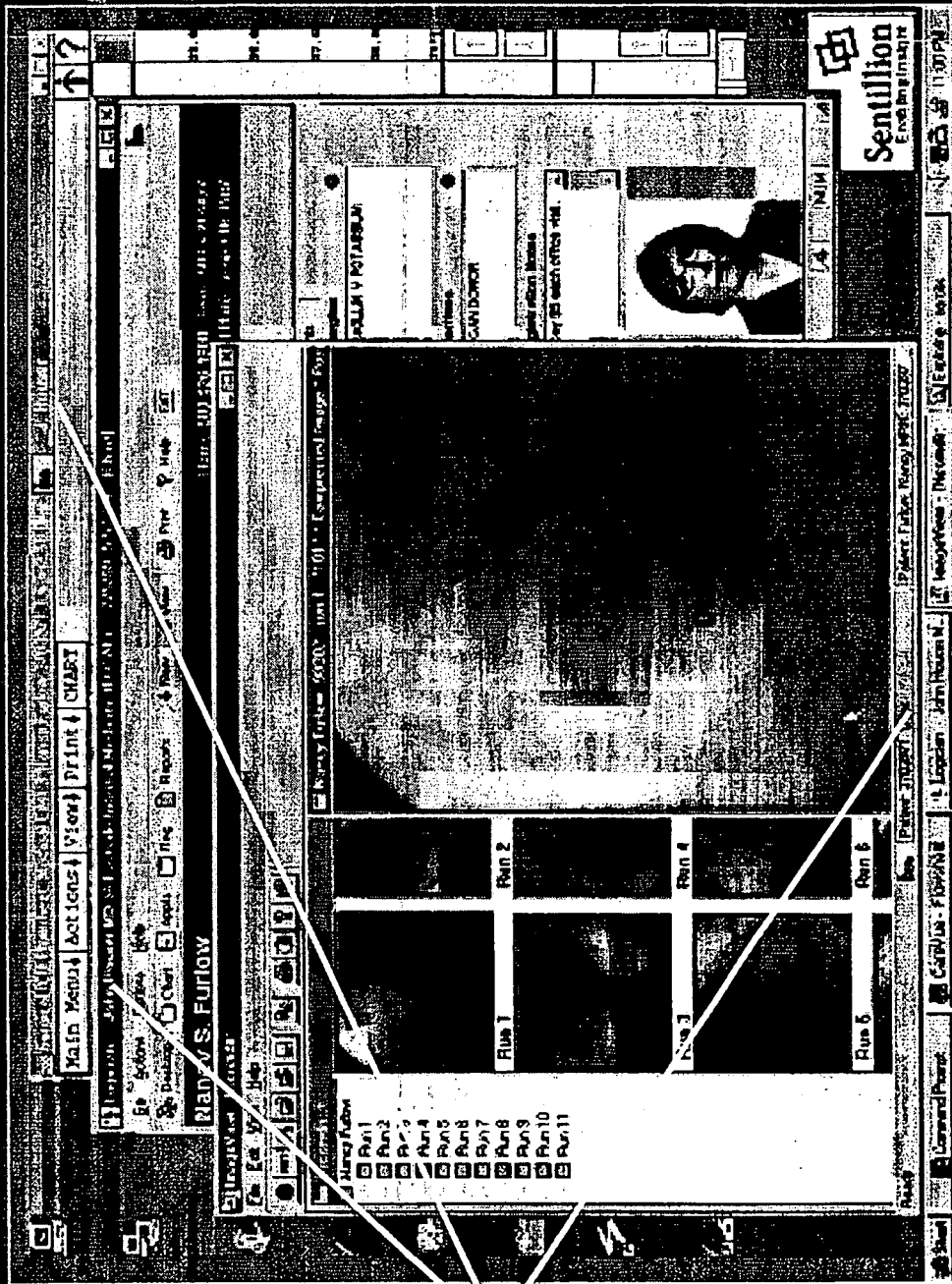
Secure Links

Copyright © 2000 Sentillion, Inc.


Sentillion
ENABLING INSIGHT

Example: User Link

Dr. John
Houser



Sentillion
Enabling Insight

Copyright © 2000 Sentillion, Inc.

User Link Requirements

- One clinical desktop, many disparate applications
- Caregivers confronted with multiple logon names and passwords
- Kiosk model: instant sign-on, instant access
- Many healthcare applications already implement own sign-on
- Upwards compatible with smartcards, biometrics, etc.
- At least as secure as existing "solutions"
- No more secure than underlying platform
- Don't assume existence of PKI (don't preclude either)
- Leverage existing context management architecture



Sentillion
ENABLING INSIGHT

User Link Non-Requirements

- Secure transmission of clinical data
- Unification of application access control

Copyright © 2000 Sentillion, Inc.



Sentillion
ENABLING INSIGHT

Context
Change
Survey

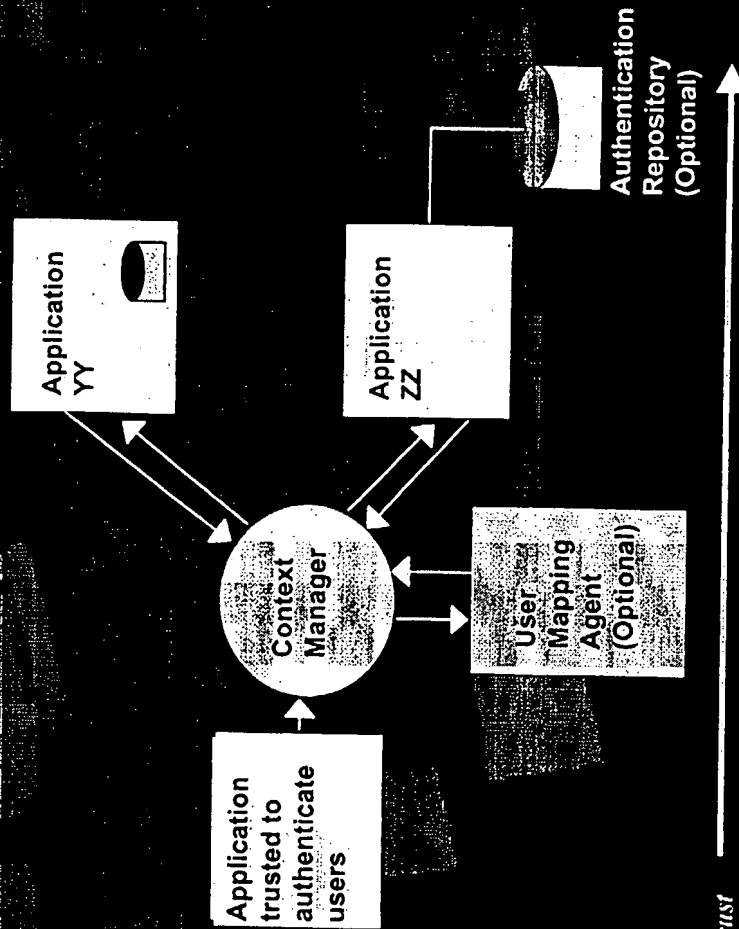


Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Theory of Operation: User Link

(1) User signs on
(enters logon
name, password,
swipes security
card, etc.)

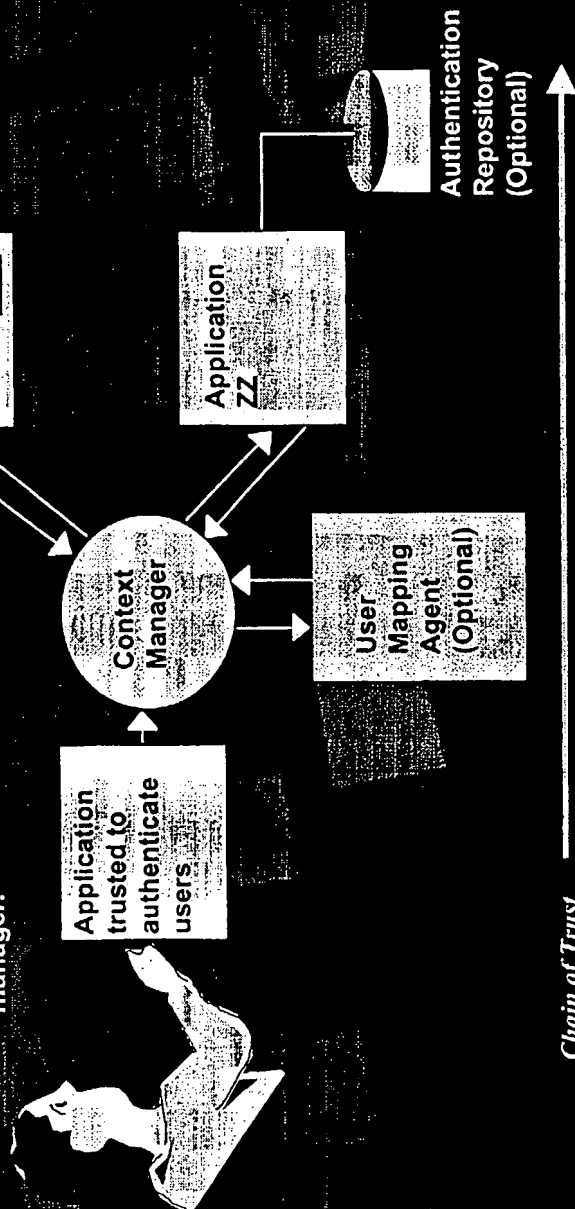


Copyright © 2000 Sentillion, Inc.

Theory of Operation: User Link

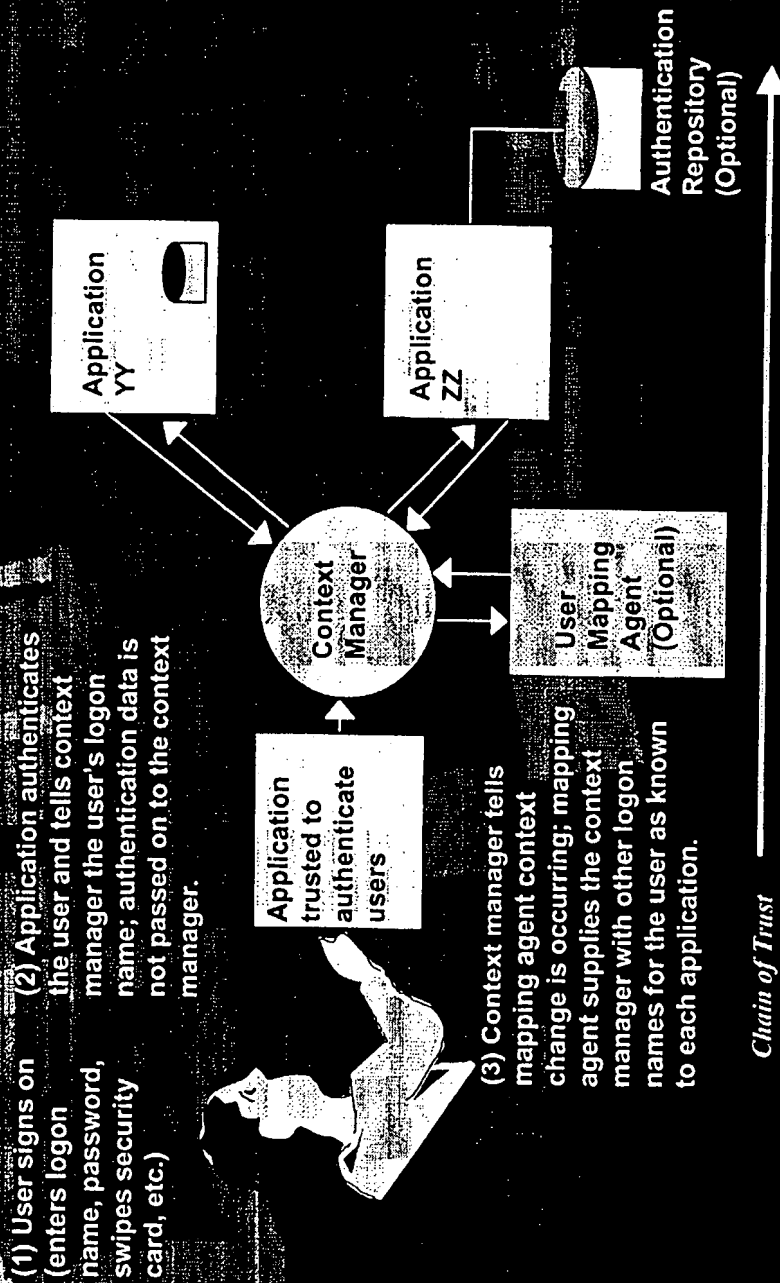
(1) User signs on (enters login name, password, swipes security card, etc.)

(2) Application authenticates the user and tells context manager the user's login name; authentication data is not passed on to the context manager.

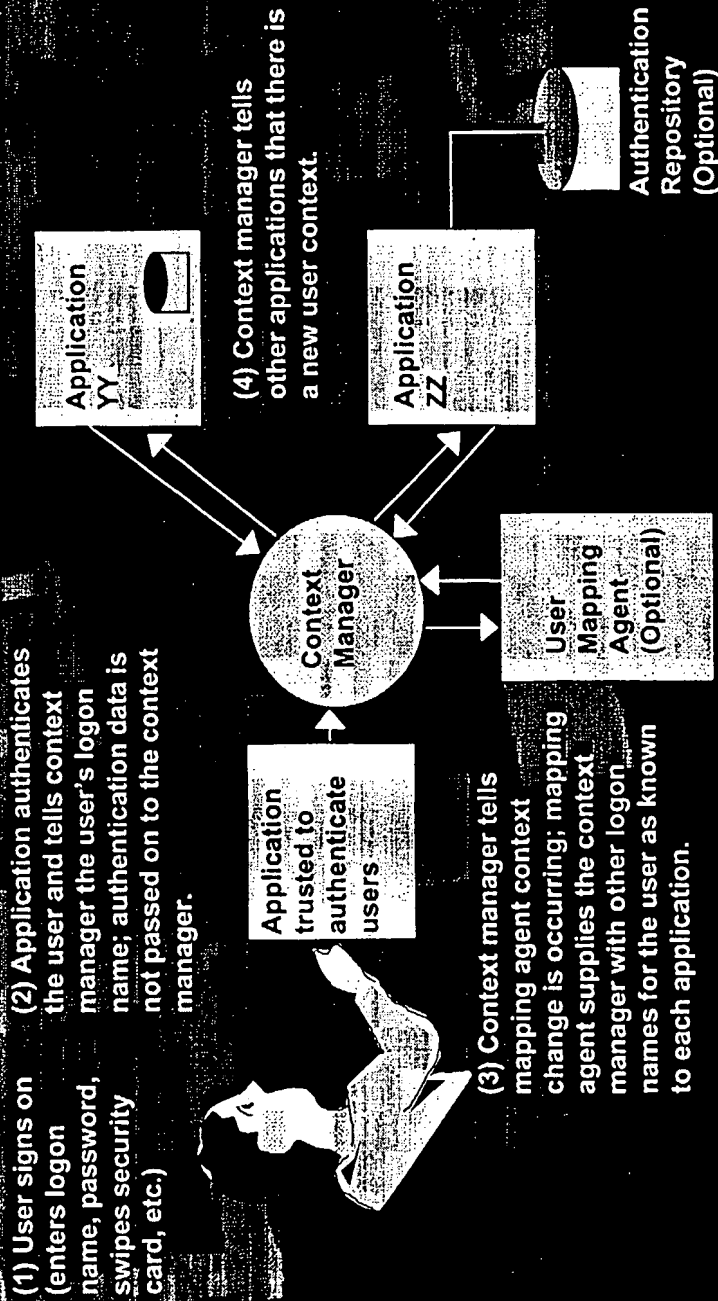


Chain of Trust

Theory of Operation: User Link

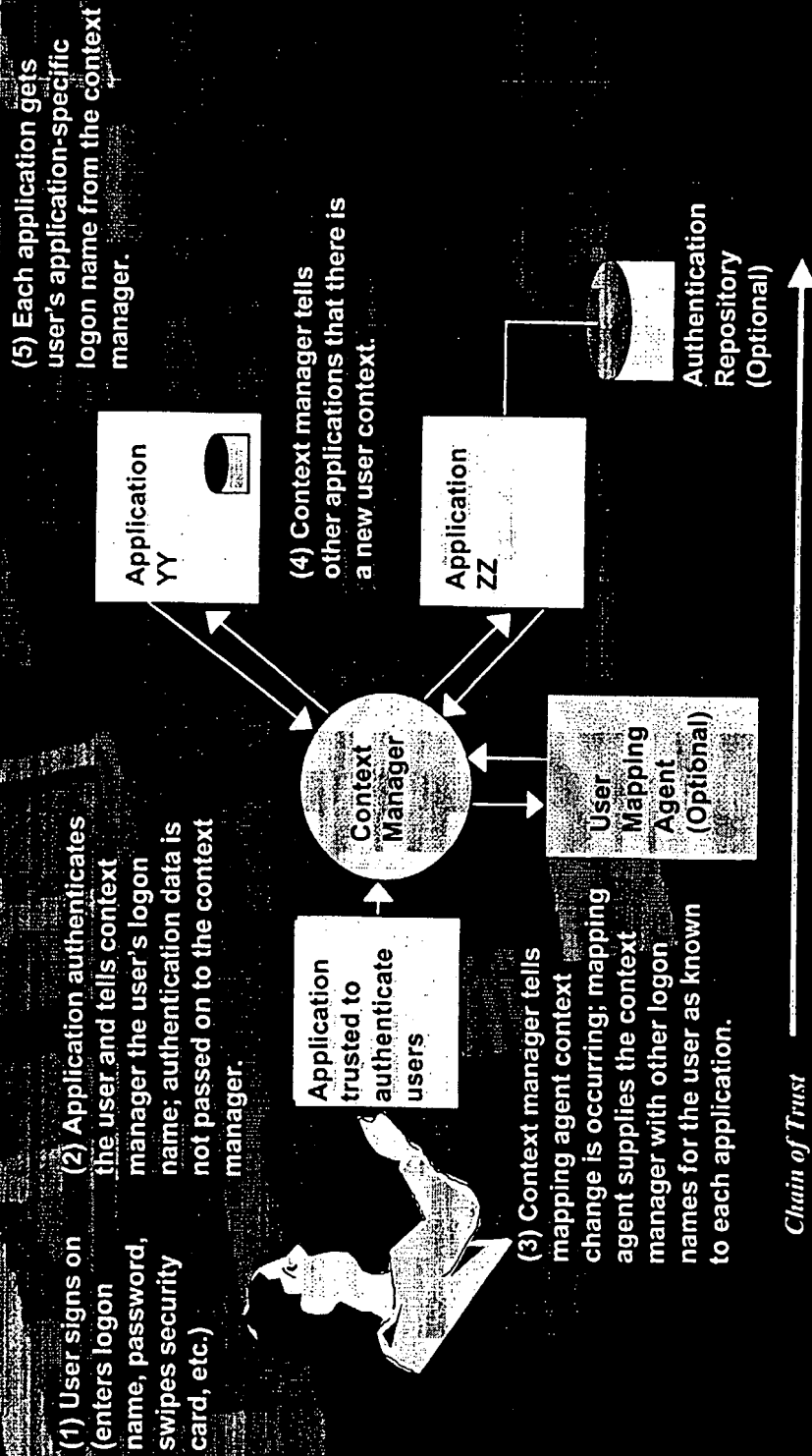


Theory of Operation: User Link



Chain of Trust

Theory of Operation: User Link



Copyright © 2000 Sentillion, Inc.

Theory of Operation: User Link

(1) User signs on (enters logon name, password, swipes security card, etc.)

(2) Application authenticates the user and tells context manager the user's logon name; authentication data is not passed on to the context manager.

Application trusted to authenticate users

(3) Context manager tells mapping agent context change is occurring; mapping agent supplies the context manager with other logon names for the user as known to each application.

Context Manager

User Mapping Agent (Optional)

Application YY

(4) Context manager tells other applications that there is a new user context.

Application ZZ

Authentication Repository (Optional)

(5) Each application gets user's application-specific logon name from the context manager.

(6a) An application optionally consults internal authentication repository to get application-specific authentication data for the new user and automatically signs-on the user.

Chain of Trust



Sentillion
ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.

Theory of Operation: User Link

(1) User signs on (enters logon name, password, swipes security card, etc.)

(2) Application authenticates the user and tells context manager the user's logon name; authentication data is not passed on to the context manager.



Application trusted to authenticate users

(3) Context manager tells mapping agent context change is occurring; mapping agent supplies the context manager with other logon names for the user as known to each application.

Application YY

(4) Context manager tells other applications that there is a new user context.

Application ZZ

(6a) An application optionally consults internal authentication repository to get application-specific authentication data for the new user and automatically signs-on the user.

(6b) An application optionally consults external authentication repository to get application-specific authentication data for the new user and automatically signs-on the user.

(5) Each application gets user's application-specific logon name from the context manager.



Authentication Repository (Optional)

Chain of Trust

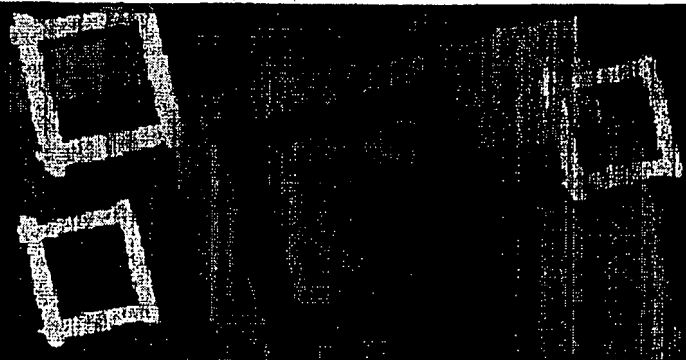
Copyright © 2000 Sentillion, Inc.



Sentillion

ENABLING INSIGHT

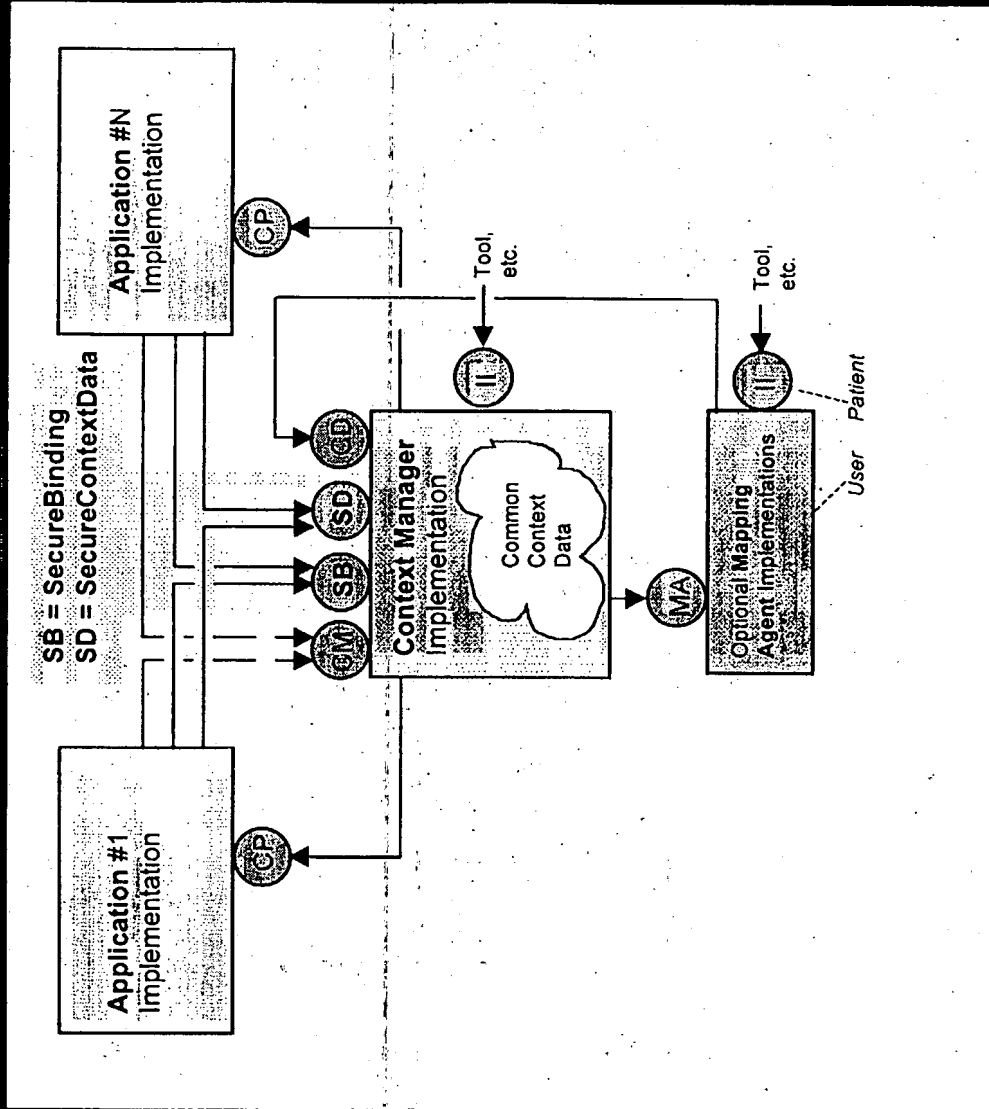
Participant
Coupon



Sentillion
ENABLING INSIGHT

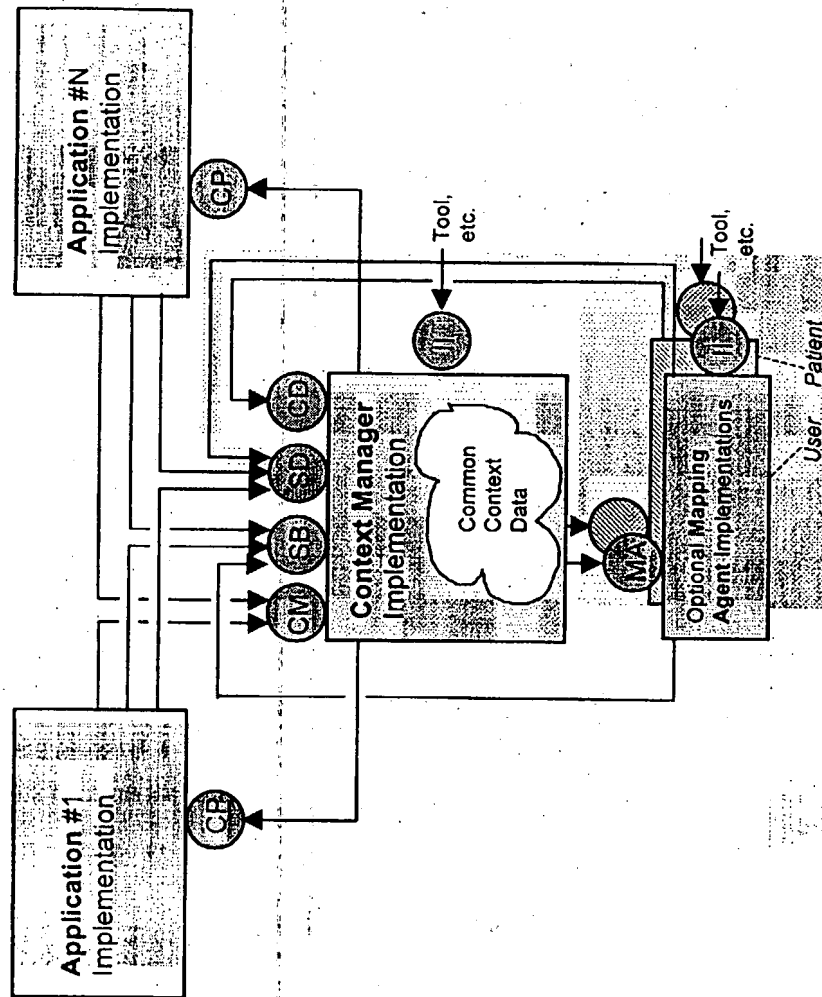
Copyright © 2000 Sentillion, Inc.

Architecture

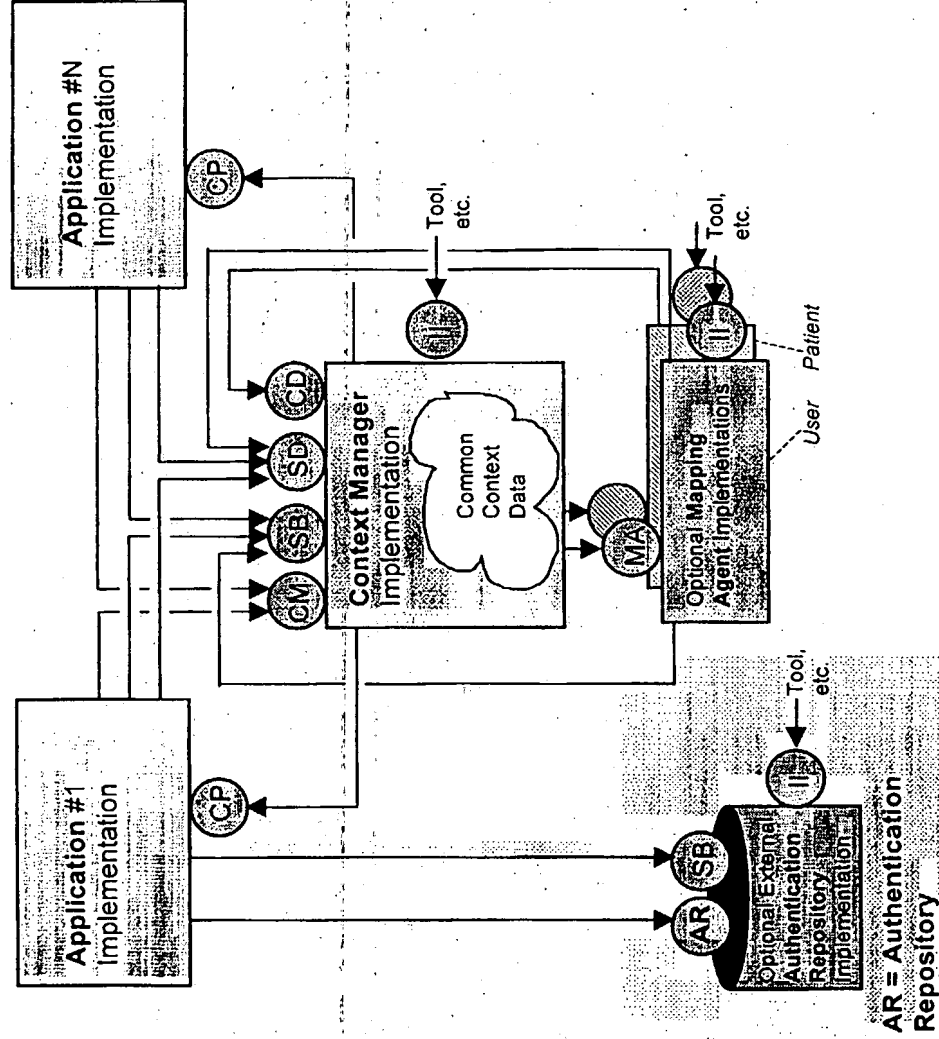


Copyright © 2000 Sentillion, Inc.

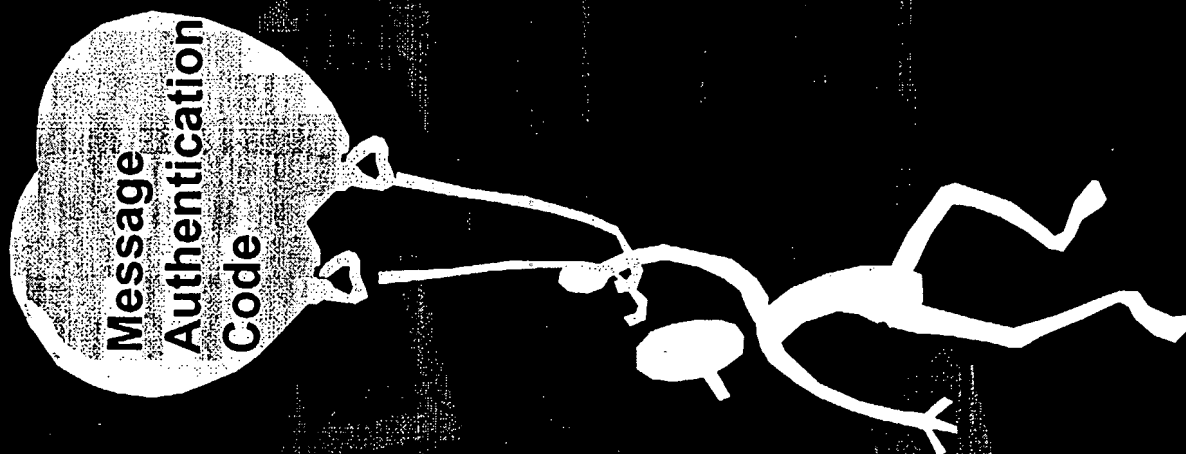
Architecture



Architecture



Copyright © 2000 Sentillion, Inc.



Copyright © 2000 Sentillion, Inc.

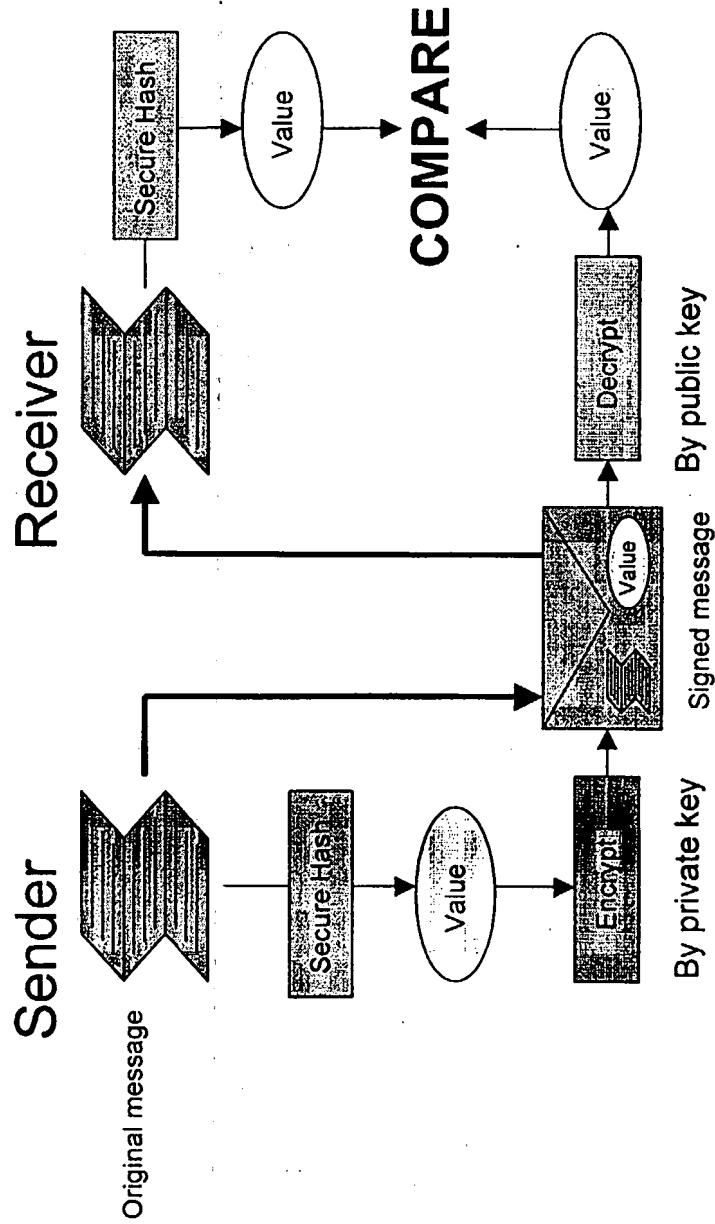

Sentillion
ENABLING INSIGHT

Secure Context Management

1. Generate public key / private key pair
2. Use "Secure Binding" process to exchange public keys
 - "Passcode" is shared secret
 - Message Authentication Code
3. Use private key to digitally sign method invocations
4. Use corresponding public key to verify methods
 - Authenticate sender
 - Ensure data integrity
5. Include a "nonce" (generally a coupon) to foil replay attacks



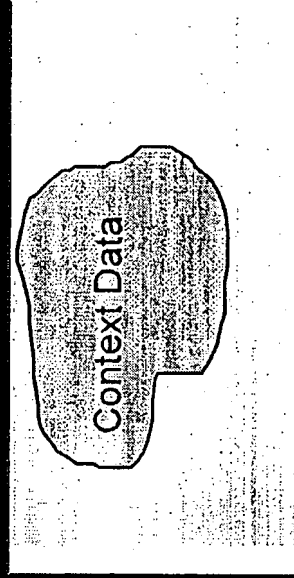
Public Key Signatures



Copyright ©Jung Joo-won, 1996, <http://simac.kaist.ac.kr/~jwjung/seminar/ssl-ca-inst/slides.en>

Interface SecureBinding

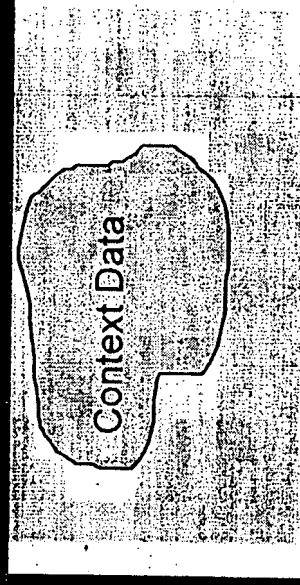
- InitializeBinding
- FinalizeBinding



Interface SecureContextData

- GetItemNames
- GetItemValues
- SetItemValues

Same as ContextData,
but with security-
related parameters



Signing Methods

ContextData

SetItemValues

inputs(long participantCoupon,
string[] itemNames,
variant[] itemValues,
long contextCoupon)

outputs()
raises(...)

GetItemValues

inputs(variant[] names,
boolean onlyChanges,
long contextCoupon)

outputs(variant[] itemValues)
raises(...)

SecureContextData

SetItemValues

inputs(long participantCoupon,
string itemNames,
variant[] itemValues,
long contextCoupon,
string appSignature)

outputs()
raises(...)

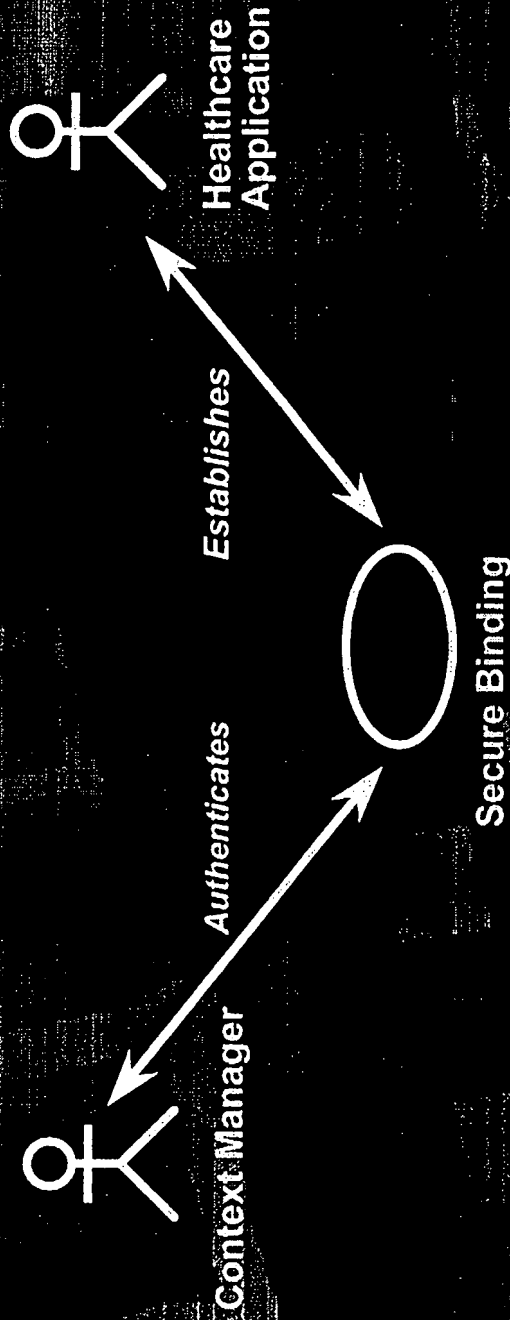
GetItemValues

inputs(long participantCoupon,
string[] names,
boolean onlyChanges,
long contextCoupon,
string appSignature)
outputs(string managerSignature,
variant[] itemValues)
raises(...)



Sentillion
ENABLING INSIGHT

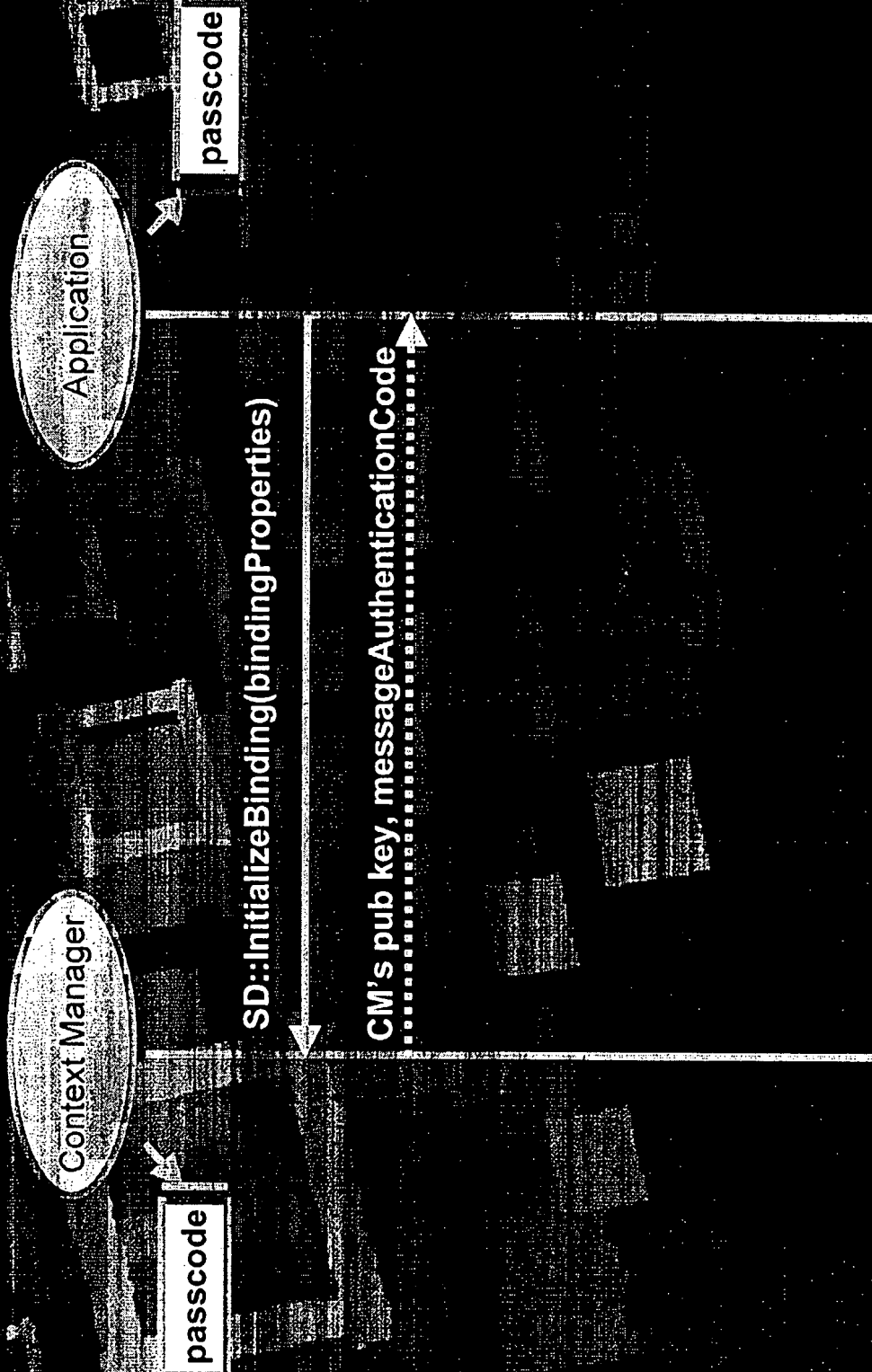
Common Context System: Establish Secure Binding Use Case



Sentillion
ENABLING INSIGHT

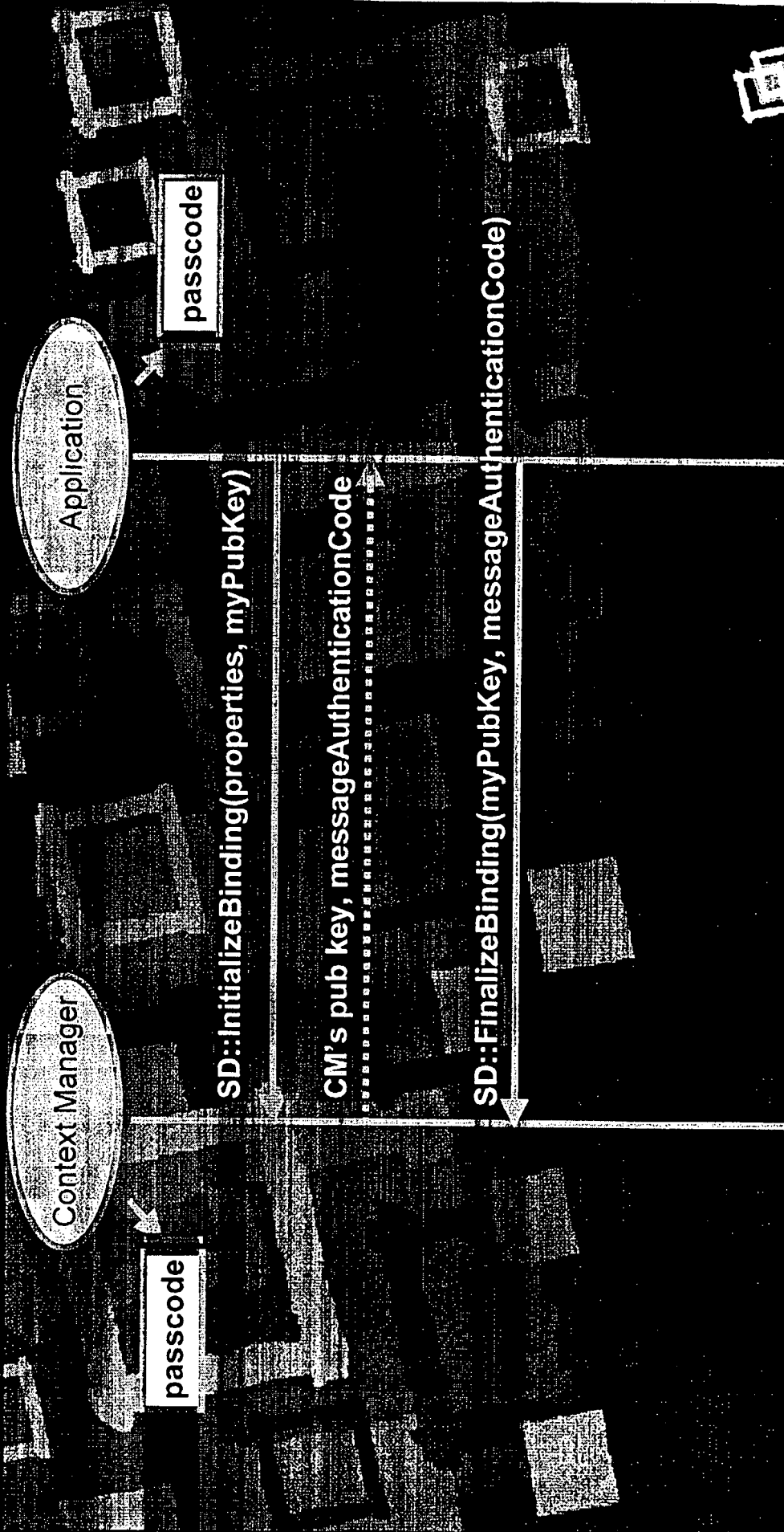
Establish Secure Binding:

initialize binding



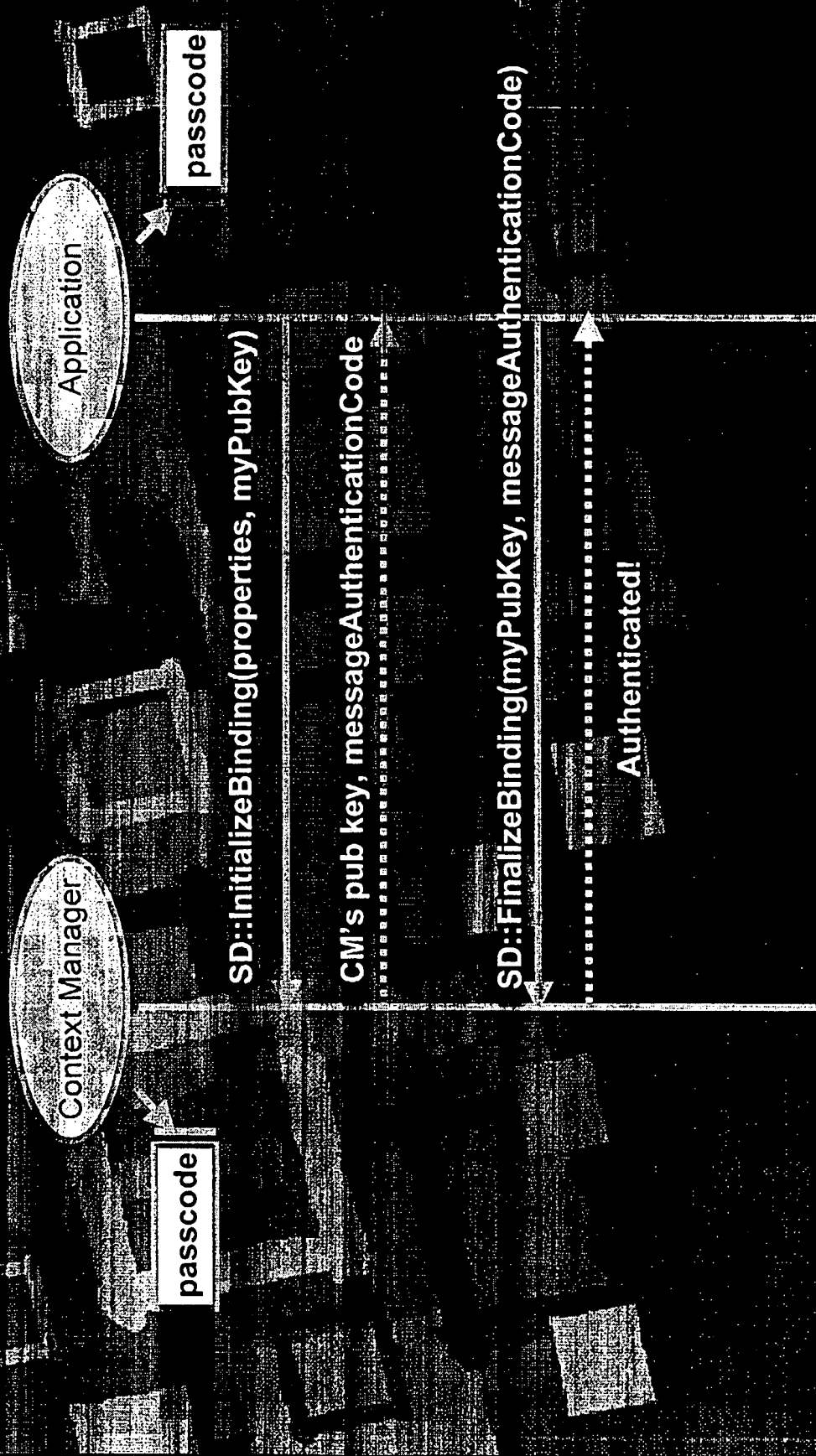
Establish Secure Binding:

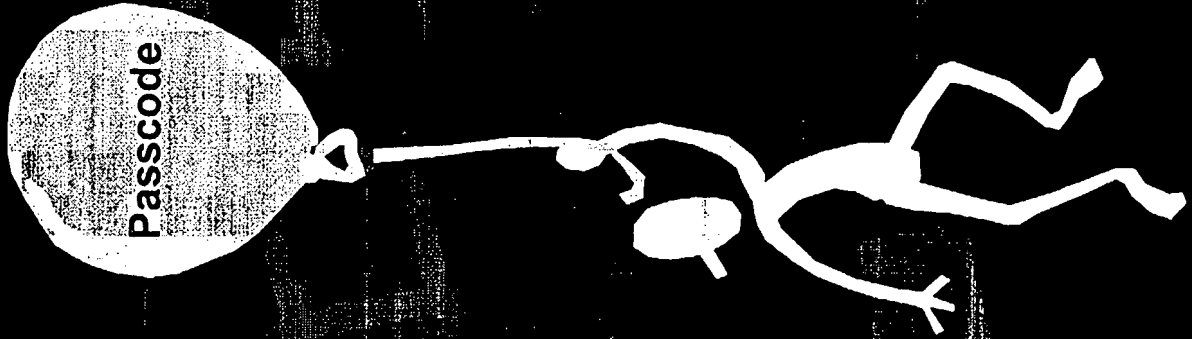
finalize binding



Establish Secure Binding:

finalize binding





ActiveX Example

Securely Set The Context

```
// C++
long contextCoupon = iCM->StartContextChanges(...);
VARIANT names = // names of items to set
VARIANT values = // values of items to set
BSTR digest = // Create message digest from coupon, item names and values
BSTR mySignature = // Sign the digest
iSD->SetItemValues(participantCoupon, names, values, contextCoupon, mySignature);
VARIANT vote = iCM->EndContextChanges(contextCoupon, ...);
BSTR decision = // Decide how to proceed --- ask user if necessary
iCM->PublishChangesDecision(contextCoupon, decision);
```



ActiveX Example

Securely Get The Context

```
// C++
VARIANT names = iSD->GetItemNames();
VARIANT values = iSD->GetItemValues(..., names, contextCoupon, ..., cmSignature);
BSTR digest = // compute digest from item values and context coupon
if (!* The digest verifies *)
{
    // It's the real context manager ...
}
```



Sentillion
ENABLING INSIGHT

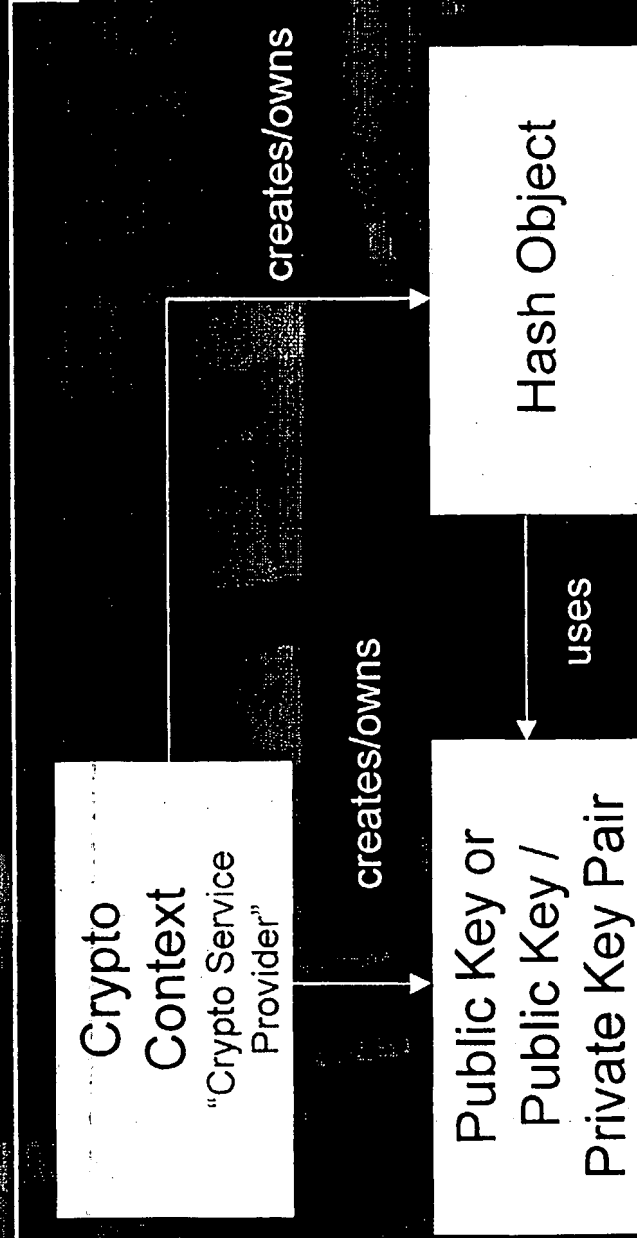
ActiveX Secure Binding

Properties for Crypto32

<u>Name</u>	<u>Value</u>	<u>Meaning</u>
Technology	CRYPTO32	Microsoft CRYPTO32 or equivalent
PubKeyScheme	RSA_EXPORTABLE	Exportable version of RSA public key / private key scheme
HashAlgorithm	MD5	MD5 secure hash algorithm (creates 128 bit hash value)

Crypto32 Summary

Crypto32 API: Create Keys, Import & Export Keys,
Compute Hash Values using Keys



Key Containers

Container created by	Container purpose	Container name
Application	Holding own key pair.	CCOW.APPLICATION-NAME.SELF
	Holding context manager's public key.	CCOW.APPLICATION-NAME.CM
	Holding authentication repository's public key.	CCOW.APPLICATION-NAME.AR
Context Manager	Holding own pair.	CCOW.CM.SELF
	Holding an application's public key.	CCOW.CM.APPLICATION-NAME
	Holding user mapping agent's public key.	CCOW.CM.MA_USER
User Mapping Agent	Holding own key pair.	CCOW.MA_USER.SELF
	Holding context manager's public key.	CCOW.MA_USER.CM
Authentication Repository	Holding own key pair.	CCOW.AR.SELF
	Holding an application's public key.	CCOW.AR.APPLICATION-NAME



Sentillion

ENABLING INSIGHT

Copyright © 2000 Sentillion, Inc.